Akademia Sztuki Wojennej

Cybersecurity and Law

Nr 1(1) 2019

Warszawa 2019

ISSN 2658-1493

Adres

Akademia Sztuki Wojennej w Warszawie
Centrum Studiów nad Cyberbezpieczeństwem
al. gen. A. Chruściela „Montera" 103
00-910 Warszawa
e-mail: cyber.law@akademia.mil.pl

Skład, druk i oprawa: Wydawnictwo Akademii Sztuki Wojennej, zam. nr 854/19, nakład 100 egz.

Spis treści

Szanowni Państwo,

oddajemy w Państwa ręce pierwszy numer nowego czasopisma. Zadaniem „Cybersecurity & Law" ma być inspirowanie do pogłębionych analiz, wymiany poglądów, stawiania pytań i poszukiwania odpowiedzi. Zakres możliwych do poruszenia tematów jest niezwykle szeroki. Postęp technologiczny sprawia, że coraz większa ilość procesów staje się wręcz niemożliwa do przeprowadzenia bez cyfrowego wsparcia. Rośnie znaczenie i dostępność Internetu Rzeczy (iOT – Internet of Things), już przeszło 10 lat temu urządzeń stale podłączonych do globalnej sieci było więcej niż ludzi, a wkrótce ich liczba może sięgnąć 50 miliardów. Stale rozwijają się mechanizmy uczenia maszynowego (machine learning) i sztucznej inteligencji (AI – artificial intelligence), a rdzeniem organizującym cyfrową rzeczywistość stanie się już niedługo sieć 5G, której komercyjne wdrożenia dopiero się rozpoczęły, podczas gdy kilka krajów, w tym oficjalnie Chiny, pracuje już nad standardem 6G. Cyfrowa rzeczywistość stała się w sposób naturalny wyzwaniem dla osób i instytucji odpowiadających za bezpieczeństwo w wymiarze krajowym i międzynarodowym. Cyberprzestrzeń to bowiem oczywiście nie tylko nowe usługi, ułatwienia, czy kanały komunikacji i rozrywka. To jednocześnie atrakcyjne środowisko do działania dla grup przestępczych i terrorystycznych, a także państw, które przy jej wykorzystaniu mogą realizować rozbudowane operacje wywiadowcze, polityczne, czy socjotechniczne oraz dokonywać swoistej projekcji siły. Działania w cyberprzestrzeni mogą być także przygotowaniem do podjęcia lub elementem trwających operacji militarnych.

Nie zaskakuje zatem, iż zgodnie z decyzjami NATO cyberprzestrzeń została uznana za domenę operacyjną działań militarnych. W deklaracji końcowej szczytu NATO, który odbył się w Walii w 2014 r. Sojusz potwierdził, iż należy mieć świadomość, że „zagrożenia i ataki cybernetyczne będą coraz częstsze, bardziej złożone i potencjalnie niszczące". Jednocześnie potwierdzono wówczas, że „obrona cybernetyczna należy do podstawowych zadań kolektywnej

obrony NATO", zwracając jednocześnie uwagę na możliwość zastosowania w przypadku ataku w cyberprzestrzeni art. 5 Traktatu Północnoatlantyckiego. Podczas szczytu warszawskiego w 2016 r. NATO potwierdziło swój mandat do obrony w tej sferze i uznało cyberprzestrzeń za obszar działań, w którym musi bronić się tak samo skutecznie jak w powietrzu, na lądzie i na morzu. Podczas szczytu NATO w Brukseli w 2018 r. podkreślono znaczenie tworzenia nowej domeny działań operacyjnych sojuszu. Zapadła też decyzja o reformie struktur dowodzenia NATO i utworzeniu Centrum Operacji Cyberprzestrzeni (ang. Cyberspace Operations Center) w Mons w Belgii wchodzącego w skład struktury dowodzenia NATO.

Podkreślenia wymaga, że cyberprzestrzeń to jedyna domena operacyjna wymyślona, stworzona i prawie dowolnie modyfikowana przez człowieka wedle jego kreatywności i potrzeb. To człowiek najlepiej zna prawa nią rządzące i potrafi wykorzystywać do swoich celów jej zalety. Operacje w cyberprzestrzeni charakteryzują się kilkoma wspólnymi cechami, które wpływają na atrakcyjność wykorzystania tej domeny. Przeprowadzenie ataku w cyberprzestrzeni jest stosunkowo tanie, szybkie, nie wymaga zaangażowania dużego zespołu, a często nie wymaga nawet samodzielnego dysponowania pogłębioną wiedzą, gdyż zlecenie odpowiednio zdefiniowanej „usługi", czy nabycie i wykorzystanie służących do wrogiego działania narzędzi nie nastręcza wielu trudności. Oczywiście istotny jest globalny charakter sieci, dzięki czemu możliwość operowania na terenie innego kraju nie wymaga fizycznej obecności na jego terytorium. W tym zakresie zmiany może przynieść wdrożenie koncepcji swoistego internetowego izolacjonizmu, czyli możliwość odcięcia się od transgranicznych węzłów komunikacyjnych, nad czym aktywnie pracuje wiele krajów, w tym Rosja, która przyjęła nawet stosowną ustawę. Cyberprzestrzeń to także cały czas stosunkowa łatwość ukrycia tożsamości, co znacząco utrudnia atrybucję, warunkującą następnie możliwość zastosowania precyzyjnej i adekwatnej odpowiedzi. Nieograniczona inwencja atakujących sprawia, że każdego dnia powstają nowe metody i narzędzia. Cechy cyberprzestrzeni jako domeny operacyjnej działają więc na korzyść tych wszystkich, którzy przy jej pomocy chcą prowadzić wrogie działania. Tym trudniejsza jest rola osób i struktur odpowiedzialnych za zapewnienie cyberbezpieczeństwa.

Także z tych powodów geostratedzy zwracają uwagę, iż charakter cyberprzestrzeni i zdolność do jej wykorzystania jako domeny operacyjnej skraca znacząco dystans między krajami na różnym poziomie rozwoju. Pozwala też na dążenie do dołączenia do grona regionalnych lub nawet globalnych potęg

krajom, które pod względem potencjału militarnego i gospodarczego nigdy nie mogłyby na to liczyć.

W Polsce kwestie dotyczące cyberbezpieczeństwa traktujemy niezwykle poważnie. To wyzwanie związane przede wszystkim z otoczeniem bezpieczeństwa kraju wschodniej flanki NATO. Bogate tradycje polskiej kryptologii, czy lwowskiej szkoły matematycznej, ale też teraźniejszość, w której możemy być dumni z międzynarodowych osiągnięć polskich uczniów, studentów, specjalistów i ekspertów w zakresie matematyki, czy informatyki, predestynują nasz kraj do odgrywania w cyfrowym świecie istotnej roli.

Na poziomie strategicznym polski rząd dokonał stosownych rozstrzygnięć. W sierpniu 2018 r. weszła w życie pierwsza polska ustawa o krajowym systemie cyberbezpieczeństwa, która stanowi, iż krajowy system opiera się co do zasady na trzech filarach: MON, ABW i NASK-PIB, odpowiedzialnych za prowadzenie działających na poziomie krajowym Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT MON, CSIRT GOV i CSIRT NASK). Ustawa określiła też zadania ministra obrony narodowej, do których należy m.in.:

– zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych – w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych;

– rozwijanie umiejętności Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych;

– pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej oraz

– prowadzenie Narodowego Punktu Kontaktowego do współpracy z NATO, którego celem ma być m.in. dział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii.

Jednocześnie, stosownie do postanowień Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022, przyjętych uchwałą Rady Ministrów z dnia 27 kwietnia 2017 r. ustalono cztery cele szczegółowe:

1) osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa;

2) wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom;

3) zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni;

4) zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

Natomiast, w zastępującej Krajowe Ramy Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, przyjętej uchwałą Rady Ministrów z dnia 22 października 2019 r. określono pięć celów szczegółowych:

1) rozwój krajowego systemu cyberbezpieczeństwa;

2) podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty;

3) zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa;

4) budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa;

5) zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

W wyniku prac zainicjowanych w MON, w marcu 2018 r. pod moim kierunkiem, powstał kompleksowy program podniesienia zdolności do działania w cyberprzestrzeni pod nazwą CYBER.MIL.PL, którego założenia przedstawiono publicznie w lutym 2019 r. Działania i zamierzenia MON ujęto w kilkudziesięciu projektach, które można tematycznie podzielić na cztery grupy:

1. Konsolidacja i budowanie struktur odpowiedzialnych za cyberbezpieczeństwo oraz zwiększenie zdolności do działania w cyberprzestrzeni.

2. Edukacja, szkolenie, trening.

3. Współpraca międzynarodowa i budowanie silnej pozycji międzynarodowej.

4. Podniesienie poziomu bezpieczeństwa resortowych i wojskowych sieci i systemów.

Jednym z projektów zidentyfikowanych w ramach drugiego filaru było także uruchomienie czasopisma naukowego poświęconego zagadnieniom cyberbezpieczeństwa. Także i ten projekt możemy wraz z wydaniem pierwszego numeru uznać za zrealizowany.

Dlaczego „Cybersecurity & Law"? Bo ważne, aby do przeszłości odeszło niesłuszne, a niestety ugruntowane przekonanie, że cyberbezpieczeństwo to domena informatyków i działów IT. Nie, zapewnienie cyberbezpieczeństwa to wyzwanie przekrojowe, które w różnym stopniu dotyka każdego z nas. To ogromny obszar, w którym rośnie zapotrzebowanie na różnego rodzaju

kompetencje, często zupełnie niezwiązane ze stricte technicznymi umiejętnościami. Analiza prawna, zarówno w zakresie prawa administracyjnego, karnego, cywilnego, jak europejskiego czy międzynarodowego, a także refleksja systemowa i organizacyjna stale towarzyszą pracom prowadzonym w ramach nowej domeny operacyjnej.

Redaktor naczelnej i całemu zespołowi czasopisma gratuluję pierwszego numeru i życzę wytrwałości, pasji i kreatywności w dążeniu do stałego doskonalenia tego niezwykle ciekawie zapowiadającego się nowego tytułu!

Tomasz Zdzikot
sekretarz stanu w MON
pełnomocnik ministra obrony narodowej
do spraw bezpieczeństwa cyberprzestrzeni

Krzysztof Andrzej Wąsowski*

Cognition of the Minister of National Defense in the scope of cybersecurity

Abstract

The study attempts to analyse the competence and task standards of the Minister of National Defense in the area of the national cybersecurity system. The author distinguishes four types of functions that the Minister of National Defense performs in the created cybersecurity system in Poland. In this system, this entity is at the same time one of the specialized bodies competent for cybersecurity, at the same time the body separate and independent from them, and the entity managing CSIRT MON and a member of the College for cybersecurity.

Key words: Minister of National Defense, jurisdiction, cognition, competence, cybersecurity, threat, nationaldefence, public administration, national system of cybersecurity, digitalinfrastructure

* Dr Krzysztof Andrzej Wąsowski, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: k.wasowski@akademia.mil.pl.

The concept of cognition – jurisdiction of the operation of a public administration body

Cognition is included in the doctrine of administrative law as the jurisdiction within which the administrative body should operate. In this approach, cognition (jurisdiction of the body's operation) is often identified with the competence of a public administration body[1].

It is worth, however, to look a bit wider on the problem of cognition (jurisdiction) of the administrative body. As proposed by Z. Cieślak "(...) the meaning of the term 'jurisdiction' goes beyond legal categories, since it concerns basics of creating administrative structures (organizational structure of the public administration is a reflection of the structure of goals and tasks and administrative matters) and the principles of their functioning (...)"[2]. According to this in the author, in its broad sense, the concept of "jurisdiction" may be characterized as "the sum, type and content of matters falling under legally unindifferent activity of the entity"[3]. On the other hand, strictly procedural jurisdiction means only a specific "scope of cases", with statutory powers that a given entity (public administration body or judicial body) should resolve[4]. Hence, the processualists associate the concept of "legal capacity of organs" with the cognition of the activity of a given authority (its jurisdiction), which they define as a kind of "set of premises determining the ability to take procedural acts in administrative proceedings", and these premises are in turn determined by procedural law norms[5].

In the classic doctrine of administrative law, the concept of "scope of activity" (properties, cognition) of a given body was usually associated with

1 Por. Z. Cieślak, *Podstawowe instytucje prawa administracyjnego* [w:] Z. Niewiadomski (red.), *Prawo administracyjne*, Warszawa 2013, s. 81.

2 Ibidem.

3 Ibidem. Ten sam autor definiuje „właściwość" z perspektywy nauki administracji (w odróżnieniu od podejścia prawniczego) jako „pojęcie opisujące statyczno-strukturalne podstawy zachowania, tzn. elementy kto i co. Naturalnie w systemie administracji państwowej określenie to jest niewystarczające i zawsze musi być dopełnione opisem elementów funkcjonalno-dynamicznych, gdyż możność działania (zdolność do działania) nigdy nie jest równoznaczna z jego dokonywaniem (dokonaniem). Te dwa faktyczne, dopełniające się aspekty zachowania znajdują swoje odzwierciedlenie w układzie normatywnym, a ściślej mówiąc – w typach norm prawnych" – zob. Z. Cieślak, *Zbiory zachowań w administracji państwowej. Zagadnienia podstawowe*, Warszawa 1992, s. 28.

4 Por. B. Adamiak, *Właściwość organów* [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 1998, s. 119–120.

5 Ibidem, s. 119.

the so-called task standards, which normalized the sphere of tasks to be carried out by a given administrative entity. This approach was associated with the normative system of a given public administration body[6]. However, only the "postulativeness" of such a position was noticed quite quickly due to the significant relationship between the activities of public administration bodies and the so-called legal forms of action. It even leads to fusion – so unique and characteristic for the branch of administrative law– procedural norms with substantive and legal norms. In such a situation, the basis for implementing the cognition of a given authority in a specific administrative matter will be a competence norm[7].

Pursuant to the constitutional rule of legalism of public authority bodies (clearly exposed in the content of Article 7 of the Constitution of the Republic of Poland[8]), the competence of a public administration body must result from the provisions of generally applicable law. Structurally, legal norms regulating jurisdiction – regardless of whether they are included in a broader, systemic or strictly procedural context – should contain four basic elements: time, place, subjective features and the object of action. The essence of the criterion of time in the reconstruction of the properties (cognition) of the operation of a public administration body is the basis for the reconstruction of "rules that update the possibility of an individualized entity at a given time"[9]. The criterion of place within the norm determining the jurisdiction is usually closely related to the rules relating to territorial divisions (both general and special). The subjective criterion should include the definition of such features of a given administrative entity, such as its legal status, organizational structure, its place in the system of organs, the way it is created, changed or abolished, and finally the whole complex of personal issues related to its functioning[10]. Finally, an extremely important

6 W taki sposób kwestię tę stawia m.in. W. Dawidowicz, *Wstęp do nauk prawno-administracyjnych*, Warszawa 1974, s. 57 lub J. Filipek, *Rola prawa w działalności administracji państwowej*, Warszawa–Kraków 1974, s. 44.

7 Podobnie J. Borkowski, *Zakres przedmiotowy kodeksu postępowania administracyjnego w świetle nowelizacji*, „Państwo i Prawo" 1980, z. 5, także: W. Dawidowicz, *Zarys procesu administracyjnego*, Warszawa 1989, s. 18.

8 Art. 7 Konstytucji RP stanowi: „Organy władzy publicznej działają na podstawie i w granicach prawa".

9 Z. Cieślak, *Zbiory zachowań…*, s. 56.

10 Z. Cieślak zwraca uwagę, że przepisy wyznaczające status prawny podmiotu pełnią w procesie aktualizacji administracji państwowej bardzo ważną funkcję, gdyż nie tylko ogólnie charakteryzują prawnie dany podmiot poprzez swoje usytuowanie na początku sekwencji przepisów rekonstruujących normy prawne, ale również sygnalizują określony

element of the norm specifying the competence (cognition) of a given public administration body is the criterion of the subject of the action, which primarily determines the activation of the entire administrative system or its element (it can be said that it determines the administrative and legal nature of the activity)[11].

The political position of the Minister of National Defense

The Minister of National Defense is a central public administration body managing the department of government administration "national defense"[12], who is also a member of the central collegiate body, which is the Council of Ministers[13]. In the light of constitutional regulations, the Minister of National Defense (listed in the relevant provisions of the Basic Law *in extenso*) performs the function of an intermediary in the exercise of sovereignty over the Polish Armed Forces by the President of the Republic of Poland in peace time[14]. Characteristically for the norms determining the jurisdiction of the Minister of National Defense is the constitution already specified time (peace time). The spatial criterion, in principle, coincides with the territory of the Republic of Poland, however, the specificity of the competence of the Minister of National Defense goes beyond the territorial framework of one state due to the competence norms relating to the extensive international activity of this government administration body. In the hierarchical structure, the Minister of National Defense has a threefold role. Firstly, the Minister of National Defense, an independent government administration body with independent competences and tasks (arising from both the Act on the office of

układ zależności normatywnych w danym systemie organów oraz ogólnie przesądzają o możliwości działania w konkretnej sytuacji" – zob. Z. Cieślak, *Zbiory zachowań…*, s. 58.

11 Por. Z. Cieślak, *Zbiory zachowań…*, s. 61.

12 Zob. art. 1 ust. 1 ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz.U. z 1996 r. nr 10, poz. 56 ze zm.), dalej: UMON.

13 Por. art. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz.U. nr 106, poz. 492 ze zm.) dalej: URM.

14 Zob. art. 134 ust. 2 Konstytucji RP, a także art. 1 ust. 1 UMON – warto zwrócić przy tym uwagę, że zarówno w treści samej Konstytucji RP, jak i w UMON nie rozstrzygnięto ani o istocie relacji pośrednictwa ministra obrony narodowej przy zwierzchnictwie prezydenta RP nad Siłami Zbrojnymi RP w czasie pokoju, ani o formach i trybach wykonywania tej relacji prawnej. Drugą – ściśle przypisaną ministrowi obrony narodowej – konstytucyjną kompetencją jest wskazane w art. 134 ust. 5 Konstytucji RP upoważnienie do wnioskowania do prezydenta RP o nadanie stopnia wojskowego określonego w ustawie.

the Minister of National Defense and the Act on Government Administration Departments[15]). Secondly, it performs the function of an entity that is part of a collegiate body, which is the Council of Ministers and thus subordinate to the leadership of the Prime Minister[16]. And thirdly, the Minister of National Defense is under the authority of the President of the Republic of Poland in the sphere of exercising authority over the Polish Armed Forces in peacetime[17] and awarding military ranks[18]. On the other hand, in the sphere of the subject of activity described in the norms determining the jurisdiction of the Minister of National Defense (apart from the task of "mediation" in the authority of the President of the Republic of Poland over the Armed Forces of the Republic of Poland in peacetime), it was reduced to performing the function of managing the department of government administration "national defense"[19].

Pursuant to the "departmental" law, the national defense department (temporarily limited – which is a kind of sensation in relation to other government administration departments – to "time of peace") includes matters of: defense of the State, the Armed Forces of the Republic of Poland, cybersecurity in the military dimension, the participation of the Republic of Polish in military undertakings of international organizations and in the field of discharging military obligations arising from international agreements, as well as the issue of offset agreements[20]. The task norm – determining the scope of activity – assigns the Minister of National Defense a wide spectrum of matters – from managing (in peacetime) the overall activity of the Armed Forces through operational, executive and personnel matters in the scope of

15 Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. nr 141, poz. 943 ze zm.), dalej: UDAR, która posługuje się pojęciem zarówno „ministra właściwego do spraw obrony narodowej" (art. 19 ust. 2 UDAR), jak i „ministra obrony narodowej" (art. 19 ust. 3 UDAR).

16 Zob. art. 148 pkt 2 Konstytucji RP, także art. 6 ust. 1 a contrario URM.

17 Art. 134 ust. 2 Konstytucji RP.

18 Art. 134 ust. 5 Konstytucji RP.

19 Zob. art. 19 ust. 1 UDAR. Warto przy tym zwrócić uwagę na swoiste zastrzeżenie ustawowe, uzależniające przypisanie tej kognicji ministrowi obrony narodowej od niezależnych kompetencji prezydenta RP lub innych organów państwowych, co stanowi jednocześnie regułę kolizyjną w przypadku wątpliwości interpretacyjnych mogących zaistnieć w przypadku tzw. skrzyżowania kompetencji poszczególnych organów.

20 Zob. art. 19 ust. 1 UDAR. Warto przy tym zwrócić uwagę na swoiste zastrzeżenie ustawowe, uzależniające przypisanie tej kognicji ministrowi obrony narodowej od niezależnych kompetencji prezydenta RP lub innych organów państwowych, co stanowi jednocześnie regułę kolizyjną w przypadku wątpliwości interpretacyjnych mogących zaistnieć w przypadku tzw. skrzyżowania kompetencji poszczególnych organów.

implementation of the defense tasks of the State, performance of obligations arising from undertaken by the Council of Ministers military commitments to perform tasks as the *statio fisci* of the State Treasury[21]. It is difficult to treat the task standards (also referred to as directional) as the standards defining cognition (jurisdiction) of a given body in the procedural sense (or closely related to it in the case of administrative law, in the substantive sense).These standards determine the content of the public administration, treating it through the prism of the function directly related to the values recognized by the legislator. The result of these norms is a kind of order imposed by the legislator on a given public administration body, that it should strive to implement the values imposed on it through legal norms (expressed in legal regulations)[22].

National Cybersecurity System

There is no doubt that in recent decades there has been a noticeable technological progress, especially in the field of ICT, having an increasing (almost decisive) impact not only on the economic life of societies, but also on the security of citizens, including defense and national security. Digital technologies bring not only huge opportunities, but also significant threats, manifested in the growing number of so-called computer incidents[23]. This situation was met at a supranational level. In particular, the European Commission together with the High Representative of the Union for Foreign Affairs and Security Policy already in 2013 presented a communication on the European Cybersecurity Strategy entitled *Open, secure and protected cyberspace*[24] together with a legislative proposal relating to the Cybersecurity Directive. Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of security of network and information systems in the territory of the Union[25] was adopted on July 6, 2016.

21 Por. art. 2 pkt 1–23 UMON.
22 Cieślak Z., *Zbiory zachowań…*, s. 63.
23 Szerzej problematyka ta została ujęta w licznych opracowaniach i raportach, jak m.in. *Krajobraz bezpieczeństwa polskiego Internetu 2016. Raport roczny z działalnościCERT Polska*, NASK, https://www.cert.pl/PDF/Raport_CP_2016.pdf.
24 Join (2013) 1 Final, 7.02.2013.
25 Dz.Urz. UE L 194 z 19.07.2016, s. 1; dalej: Dyrektywa 2016/1148.

The regulation imposed on all Member States the creation of a system capable of guaranteeing the required level of cybersecurity of the information systems in the service sectors of key importance for maintaining critical socio-economic activities, such as energy, transport, banking, financial institutions, health sector, water supply and digital infrastructure. The instrument intended to support and coordinate the functioning of the entire system is a specific administrative system of specialized public administration bodies and related administrative entities (such as computer incidents response teams[26]) operating on the basis of the single point of contact for cybersecurity issues. Directive 2016/1148 set the European Union Member States time to implement its provisions by May 9, 2018 (except that it is an example of the so-called minimum harmonization, not limiting Member States to extend the level of cybersecurity required by the Directive).

Poland, in fulfilling the obligations imposed on it by the aforementioned directive, began legislative activities in April 2017, when the Council of Ministers adopted resolution No. 52/2017 adopting a strategic document on cyberspace in the form of the National Cybersecurity Policy Framework of the Republic of Poland for 2017–2022. At that time, work began on the draft law implementing Directive 2016/1148 in the Ministry of Digitization. On January 8, 2018, the process of interdepartmental arrangements and consultations was commenced[27], closed with the decision of the Council of Ministers, directing the works on the bill to the Parliament[28]. On April 30, 2018, the bill was submitted to the Sejm[29], which on July 5, 2018 adopted the Act on the national cybersecurity system[30].

The purpose of the Act, which entered into force on August 28, 2018, was primarily to organize and define the functioning of the national cybersecurity system[31]. The implementation of the statutory goal was achieved by covering

26 CSIRT – Computer Security Incident Response Teams.

27 A detailed course of this process together with the documentation can be found at the website of the Government Legislation Center – https://legislacja.rcl.gov.pl/projekt/12304650/ katalog/12466714#12466714.

28 See The Memorandum of Understanding no. 17/2018 of the meeting of the Council of Ministers on April 26, 2018 (RM-000-17-18) – https://legislacja.rcl.gov.pl/docs//2/12304650/12466740/124 66745/dokument341423.pdf.

29 Drukowi sejmowemu nadano nr 2505. Szczegółowy przebieg prac parlamentarnych zob. http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2505.

30 Dz.U. z 2018 r., poz. 1560; dalej: UKSC.

31 Zob. Ocena skutków regulacji do projektu ustawy o krajowym systemie cyberbezpieczeństwa – https://legislacja.rcl.gov.pl/projekt/12304650/katalog/12466714#12466714.

the indicated sectors of the national economy with direct regulatory effect, defining criteria for the separation of key service operators, determining the minimum ICT security requirements for information systems of key service operators and digital service providers, as well as establishing statutory cybersecurity requirements and obligations for teams responding to computer security incidents. There is no doubt that from a praxeological point of view for the smooth functioning of the system (administrative system), the test of implementation of the control method and the exercise of supervisory functions by the public administration bodies appointed for this purpose will be crucial, regardless of whether they have acquired such status in the political sense or only functional.

The taxonomy of the Act was built on a model characteristic for regulatory legislation of linking a specific constitutional system of various categories and functions of public administration bodies and other administrative entities with the assignment of tasks correlated with the obligations specified in the Act of administered entities. Traditionally, the legislator has separated control powers (linking them a little over the top with the control powers) to authorized employees of broadly understood administrative entities. A relatively modern sanction system was also introduced in the form of financial administrative penalties, which will undoubtedly increase the weight and "effectiveness" of control proceedings. In turn, the "criminal and administrative" procedure will necessarily become the basic instrument for the implementation of supervisory competences (*ex post*), which, in conjunction with the ex-ante supervision instruments (in particular permitting decisions), should give a wide range of regulatory tools to effectively stimulate behaviour of the entities functioning on the given relevant markets.

Competency standards of the Minister of National Defense under the National Cybersecurity System

As noted by Z. Cieślak, „normy kompetencyjne pełnią z racji swojego umiejscowienia w ciągu norm prawnych rolę czynnika limitującego prawnie ingerencję organów państwowych, regulując podmiotowy i przedmiotowy zakres zastosowania danej formy działania. Odnoszą się zatem bezpośrednio do funkcji działającego podmiotu, wpływają na zakres jego aktywności, a warunkiem ich stosowania jest uprzednia rekonstrukcja norm określających

właściwość i norm regulujących prawne formy działania”[32]. Such a structure, concerning a kind of balance between what is structural and what is functional in administration[33], is essentially to set the subject-subject boundaries of the formal activity of administrative entities, which in turn leads to the conclusion that the competence standards are closely related to legal forms of activity[34]. Thus, the review of competence norms of the Minister of National Defense will be carried out from the point of view of competence norms identified with legal forms of activity.

In the light of the Act on the national cybersecurity system, the Minister of National Defense has been described in at least four basic political systems.

First of all, being an element of the national cybersecurity system, as the competent authority in these matters[35], secondly, as an independent coordination, control and management body in the scope of competences separately assigned to it by the legislator[36], and thirdly, as the authority managing[37] the Computer Security Incident Response Team operating at the national level (CSIRT MON), fourthly as a member of the collegiate body (College) which is the consultative and advisory body of the Council of Ministers in the cybersecurity matters[38].

It should be added that the adoption of the Act on the national cybersecurity system also introduced a change in the Acton government administration departments[39], separating somehow the subdivision of “cyberspace security” into functioning in the “civil dimension” (assigning this element to the section “digitization”)[40] and operating in the “military dimension” (assigning this element to the “national defense” section)[41].

As it has been mentioned above, the Minister of National Defense is an element of the national security system due to the fact that he has been indicated in the act as the authority competent for cybersecurity: 1) for

32 Z. Cieślak, *Zbiory zachowań…*, s. 75.
33 Por. J. Borkowski, *Zagadnienie kompetencji ogólnej i szczegółowej w prawie administracyjnym*, „Studia Prawnicze” 1971, nr 3.
34 Związek ten jest tak ścisły, że jak twierdzi Z. Cieślak, „normy kompetencyjne mają charakter ius cogens” – zob. Z. Cieślak, *Zbiory zachowań…*, s. 75.
35 Zob. art. 4 pkt 17 w zw. z art. 41 pkt 6, 9 oraz 11 UKSC.
36 Por. rozdz. 10 UKSC.
37 Tak wprost stanowi treść art. 2 pkt 2 UKSC.
38 Zob. art. 64 w zw. z art. 66 ust. 1 pkt 4 ppkt c) UKSC.
39 Zob. art. 78 UKSC.
40 Zob. art. 12a ust. 1 pkt 10 UDAR.
41 Zob. 19 ust. 1 pkt 1a UDAR.

the health care sector – including entities subordinate to or supervised by the Minister of National Defence, including entities whose ICT systems or ICT networks are covered by a uniform list of objects, installations, devices and services included in the critical infrastructure[42], as well as including entrepreneurs with special economic and defence significance, in relation to which the Minister of National Defense is the organizing and supervising body for performing the defence tasks[43]; 2) for the digital infrastructure sector – for the entities specified in the same manner[44]; 3) for digital services providers – covering the same entities as specified above[45]. In the indicated sectors and toward the indicated digital services providers, the legislator assigns to the Minister of National Defense, on account of having the status of "the cybersecurity competent authority" authoritative (imperial) competences, which include in particular: 1) competence to issue decisions on the recognition of the entity as a key service operator[46]; 2) competence to issue a decision confirming the expiry of the decision on recognition as a key service operator[47]; 3) establishing a cybersecurity team for a given sector or subsector[48] (with the exception that, as part of exercising this competence, the competent authority for cybersecurity is required to provide information to operators of key services in a given sector and to CSIRT MON, CSIRT NASK and CSIRT GOV)[49]; 4) competence to impose administrative fines[50], which are instruments of supervision exercised against key service operators and digital service providers, and in specific situations also towards the key service operator's manager[51]. In addition to the clearly defined powers of authority of the Minister of National Defense as the authority competent for cybersecurity, the legislator assigned a whole range of competences (presented in the form

42 Zob. art. 41 pkt 6 w zw. z art. 26 ust. 5 UKSC w zw. z art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.
43 Zob. art. 41 pkt 6 w zw. z art. 26 ust. 5 UKSC w zw. z art. 5 pkt 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców.
44 Zob. art. 41 pkt 9 w zw. z art. 26 ust. 5 UKSC.
45 Zob. art. 41 pkt 11 w zw. z art. 26 ust. 5 UKSC.
46 Zob. art. 5 ust. 1 w zw. z art. 42 ust. 1 pkt 2 UKSC.
47 Zob. art. 5 ust. 6 w zw. z art. 42 ust. 1 pkt 2 UKSC.
48 Zob. art. 44 ust. 1 UKSC.
49 Zob. art. 44 ust. 4 UKSC.
50 Zob. art. 53 ust. 2 pkt 2 w zw. z art. 74 ust. 1 UKSC.
51 Zob. art. 75 UKSC.

of "tasks" imposed on this authority) of a non-executive, material-technical or organizational nature resulting from control and information tasks[52].

The legislator assigned a separate group of tasks to the Minister of National Defense as a specialized, autonomous public administration body, separated in the Act on the national cybersecurity system[53]. As part of these tasks, the Minister of National Defense was assigned various competences, both in the scope of implementing "imperious"[54] legal forms of action, and those of a "non-empowering" nature-controlling[55] or *strictly* organizational[56] or material-technical[57].

It is difficult to see *the ratio* of specific separation of the political position of the Minister of National Defense, especially in the context of his location among the authorities responsible for cybersecurity, where the tasks and

52 Przykłady takich zadań-uprawnień-obowiązków znajdziemy choćby w treści art. 42 ust. 1 UKSC, gdzie ustawodawca zawarł możliwość „powierzenia realizowania w jego imieniu niektórych zadań (…) jednostkom podległym lub nadzorowanym przez ten organ" (art. 42 ust. 3 UKSC), w formie „porozumienia" (art. 42 ust. 4 UKSC), w którym winny zostać określone „zasady sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym wykonywaniem powierzonych zadań" (art. 42 ust. 5 UKSC). W kwestiach analizy doktrynalno-teoretycznej koncepcji porozumienia administracyjnego jako prawnej formy działania organów administracji publicznej zob. Z. Cieślak, *Porozumienie administracyjne*, Warszawa 1982.

53 Zob. rozdział 10 UKSC – „Zadania ministra obrony narodowej".

54 Chociażby kompetencja zwierzchnia do kierowania działaniami związanymi z obsługą incydentów w czasie stanu wojennego (zob. art. 51 pkt 5 UKSC), czy też prowadzenie Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu Północnoatlantyckiego (zob. art. 52 UKSC).

55 W szczególności: pozyskiwanie narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej (zob. art. 51 pkt 4 UKSC), ocenę wpływu incydentów na system obrony państwa (zob. art. 51 pkt 6 UKSC), ocenę zagrożeń cyberbezpieczeństwa w czasie stanu wojennego (zob. art. 51 pkt 7 *in principio* UKSC), czy też rozwijanie systemów wymiany informacji o zagrożeniach cyberbezpieczeństwa w obszarze obrony narodowej (zob. art. 52 pkt 4 UKSC).

56 M.in.: współpraca Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa (zob. art. 51 pkt 1 UKSC), zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych (zob. art. 51 pkt 2 UKSC), rozwijanie umiejętności Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych (zob. art. 51 pkt 3 UKSC), rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej (zob. art. 51 pkt 4 UKSC).

57 Jak choćby udział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii (zob. art. 52 pkt 5 UKSC) lub przedstawianie właściwym organom propozycji dotyczących działań obronnych (zob. art. 51 pkt 7 *in fine* UKSC).

competences of this minister in the military-defense sphere were clearly indicated.

The explanatory memorandum to the draft Act on the national cybersecurity system contains only a brief explanation indicating that "the introduction to the draft Act of a separate chapter on the tasks of the Minister of National Defense aims to take into account its role in the process of supervision over the state's cyber defense, regulating responsibility for the military sphere of the national cybersecurity system and taking into account the functioning of this system during the period of martial law"[58]. It is hard not to get the impression that instead of clarifying possible interpretative doubts, justification of introducing the said separation by the Minister of National Defense formulated in such a way multiplies them even more[59].

A surprising way of creating the competences of the Minister of National Defense is to leave a kind of interpretation gap in the relations of this body with the newly created entity, which is CSIRT MON. In principle, apart from the casual competence assigned to the Minister of National Defense in the regulation defining the "management" of CSIRT MON, the legislator does not regulate the mutual relations of these two entities, which are key to the efficiency of the cybersecurity system in the area of defense. The issues of the political status of the CSIRT MON go beyond the scope of this study.

On the other hand, it is not surprising not to assign any separate powers to the Minister of National Defense as a member of a collegiate body, which is the Cybersecurity College situated as an opinion-making and advisory body of the Council of Ministers, because such "lack" results from the very essence of the collegiate body, within which separate competences are assigned only to chairmen of such bodies[60].

58 Zob. Uzasadnienie do projektu ustawy o krajowym systemie cyberbezpieczeństwa – Sejm RP VIII kadencji, druk nr 2505.

59 Choćby z uwagi na fakt, że nie wszystkie zadania – kompetencje (ba, nawet ich zdecydowana mniejszość) zawarte w art. 51 i 52 UKSC odnoszą się do stanu wojennego. Dodatkowo komplikacje interpretacyjne może powodować przypisywanie specjalnych kompetencji na czas stanu wojennego ministrowi obrony narodowej w sytuacji i tak sporego zamętu kompetencyjnego wprowadzonego postanowieniami Konstytucji RP w zakresie sposobu sprawowania zwierzchności nad Siłami Zbrojnymi RP i szeroko rozumianą polityką obronną państwa między takimi naczelnymi organami administracji państwowej, jak prezydent Rzeczypospolitej Polskiej, Rada Ministrów, prezes Rady Ministrów czy właśnie minister obrony narodowej.

60 Bodaj najbardziej charakterystycznym przykładem takiego „funkcjonowania" w ramach organu kolegialnego jest przewodniczący Krajowej Rady Radiofonii i Telewizji, będący jednocześnie przewodniczącym organu kolegialnego, jakim jest Krajowa Rada Radiofonii

Summary

It is hard to resist the impression that the multitude and diversity of competences assigned to the Minister of National Defense under the national cybersecurity system may in practice lead the operation of this supreme (constitutional) public administration body to various interpretative doubts, which in the undoubtedly highly responsible (directly related to state security) role, which this body performs in the public administration system may have unpredictable consequences.

In the sphere of state security, particular emphasis should be placed on building such legal relations that will be an efficient instrument in quickly making accurate, key decisions. They should be characterized by the maximum elimination of doubts about interpretation and preventing the crossing of individual tasks and competences. In the area of cybersecurity, the legislator only to a small extent specifies the tasks imposed on the Minister of National Defense, assigning them specific legal instruments in the form of appropriate legal forms of operation. Of course, there is still the organ's practice of the body's operation, which is capable to resolve and eliminate many interpretational doubts.

Bibliography

Literature

Adamiak B., *Właściwość organów* [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 1998.

Borkowski J., *Zagadnienie kompetencji ogólnej i szczegółowej w prawie administracyjnym*, „Studia Prawnicze" 1971, nr 3.

Borkowski J., *Zakres przedmiotowy kodeksu postępowania administracyjnego w świetle nowelizacji*, „Państwo i Prawo" 1980, z. 5.

Cieślak Z., *Podstawowe instytucje prawa administracyjnego* [w:] Z. Niewiadomski (red.), *Prawo administracyjne*, Warszawa 2013.

Cieślak Z., *Porozumienie administracyjne*, Warszawa 1982.

Cieślak Z., *Zbiory zachowań w administracji państwowej. Zagadnienia podstawowe*, Warszawa 1992.

Dawidowicz W., *Wstęp do nauk prawno-administracyjnych*, Warszawa 1974.

Dawidowicz W., *Zarys procesu administracyjnego*, Warszawa 1989.

Filipek J., *Rola prawa w działalności administracji państwowej*, Warszawa–Kraków 1974.

i Telewizji, a jednocześnie posiadający odrębne niezależne władcze kompetencje do wydawania decyzji koncesyjnych w ramach postępowania prowadzonego niejako wspólnie (w swoistym współdziałaniu) z Krajową Radą in corpore.

Legal acts

Ustawa z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz.U. z 1996 r. nr 10, poz. 56 ze zm.).
Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. nr 141, poz. 943 ze zm.).
Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz.U. nr 106, poz. 492 ze zm.).

Kognicja ministra obrony narodowej w zakresie cyberbezpieczeństwa

Streszczenie

Opracowanie podejmuje próbę analizy norm kompetencyjnych i zadaniowych ministra obrony narodowej w zakresie krajowego systemu cyberbezpieczeństwa. Autor wyróżnia cztery rodzaje funkcji, jakie w kreowanym ustroju cyberbezpieczeństwa w Polsce pełni minister obrony narodowej. Podmiot ten jest w tym systemie jednocześnie jednym z wyspecjalizowanych organów właściwych do spraw cyberbezpieczeństwa, a jednocześnie odrębnym i niezależnym od nich organem, prowadzącym CSIRT MON oraz członkiem Kolegium do spraw cyberbezpieczeństwa.

Słowa kluczowe: minister obrony narodowej, właściwość, kognicja, kompetencja, cyberbezpieczeństwo, zagrożenie, obrona narodowa, administracja publiczna, krajowy system cyberbezpieczeństwa, inftrastruktura cyfrowa

Agnieszka Brzostek*

The policy of protecting public administration cyberspace based on the example of the government administration authorities indicated in the Act on the National Cybersecurity System

Abstract

The necessity of the implementation of the NIS directive resulted in the adoption of solutions and concepts which would regulate the system of cybersecurity in the cyberspace to the Polish legal order. The directive formulates the obligations to ensure cybersecurity of the information systems in the service sectors which have a key meaning for maintaining critical socio-economic activity and thus energy, transport, banking, financial institutions, the health sector, water supplies and digital infrastructure. The act on the national system of cyber-security, which implements the directive, introduces a new concept to the Polish legal order, and thus a key service operator, digital service provider, and defines the organs responsible for cybersecurity, formulating their scope of tasks and mutual relations.

Key words: national system of cyber security, Government Plenipotentiary for cybersecurity, government administration, digital infrastructure, digital services, threat, security

* Dr Agnieszka Brzostek, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: brzostek.agnieszka@gmail.com.

Preparation of the Act on the national Cybersecurity system[1] was justified by the constantly growing influence of ICTs on the socio-economic development of the European Union Member States. The increase in their use means that the products and services offered are now increasingly dependent on cybersecurity. The developed ICT system, including operations on large data resources, serves the development of communication, trade, transport and constitutes the basis for the functioning of key, digital and public administration services[2]. Therefore, any disruption of this process, whether global or local, will have an impact on the functioning and provision of services, e.g. in the public sector. Bearing in mind the above-mentioned threats, the Ministry of Digitization, as the petitioner of the bill, indicated the necessity of undertaking works on the comprehensive development of the system in the situation of constantly growing and dynamically developing threats in cyberspace. The second impulse was the need to implement into the Polish legal order the Directive of the European Parliament and of the Council (EU) 2016/1148 on the measures for a high common level of security of network and information systems on the territory of the Union (hereinafter the NIS Directive)[3], which was adopted on July 6, 2016. This forced the legislator to create the national system of the government administration authorities and equip the existing ones with new tasks and competences within the scope of implementation of activities in the area of cyber security system. Hence, the need to analyse system solutions and the scope of tasks of government administration authorities indicated in the Act on the national cybersecurity system with the solutions already adopted and implemented in this regard.

Thus, in the beginning the concept of cyberspace needs to be clarified. Limited to the basic conceptual scope only, cyberspace[4] is a space for the processing and exchanging of information created by the communication and information systems defined in Article 3 clause 3 of the Act of February 17,

1 Ustawa z dnia 8 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

2 Uzasadnienie do projektu ustawy o krajowym systemie cyberbezpieczeństwa przygotowane przez Ministerstwo Cyfryzacji, s. 1; dostępne online.

3 Dz.Urz. UE L 194. s. 1.

4 Art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2017 r., poz. 1932). Taka sama definicja w art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2017 r., poz. 1928) i w art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558 ze zm.).

2005 on the computerization of the activities of the entities performing public tasks[5], including the links between them and relations with the users. The same definition is repeated in each emergency act. A. Szmyt emphasized that the concept of cyberspace defined in this way is an indeterminate *concept, which appears in the public consciousness as a default concept, with an undetermined normative content, and is a rather colloquial conceptual cluster*[6]; in order to avoid repeating the same definitions, reference should be made to one definition given in one legal act. According to J. Wasilewski, cyberspace is a logically separated area, a digital domain for the processing and exchanging of information. This space, having a transnational character, is created by communication and information systems connected via telecommunications networks, including networks whose infrastructural elements are located in other countries. Cyberspace activity is not limited to the exchange of information only. It may also consist of merely making, modifying or simply reading[7] them. As noted by K. Chałubińska-Jentkiewicz, cyberspace should be treated as a general good enabling the development and undisturbed functioning of the information society. This is due to the fact that cyberspace already covers practically all areas of activity of both human and businesses as well as of the state itself[8].

The need to implement the NIS directive has resulted in the adaptation to the Polish legal system of solutions and concepts that will regulate the cybersecurity system in cyberspace. The directive obliged all EU Member States to guarantee the minimum level of the national cybersecurity capabilities by establishing competent authorities and a single point of cybersecurity,

5 Dz.U. z 2017 r., poz. 1897. Tak skonstruowana definicja została powtórzona także w innych aktach prawnych, np. Polityka ochrony cyberprzestrzeni RP z dnia 25 czerwca 2013 r.

6 A. Szmyt, *Opinia prawna do przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (druk sejmowy nr 4355 dostępny online).

7 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 231.

8 K. Chałubińska-Jentkiewicz szerzej opisała zjawisko cyberprzestrzeni w porządku międzynarodowym i krajowym. Szerzej: K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii*, Warszawa 2015, s. 61–72. Na ten temat pisała M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeń we współczesnym polskim porządku prawnym*, „Przegląd Prawa Handlowego" 2012, nr 2, s. 19–38, a także J. Skrzypczak, *Polityka ochrony cyberprzestrzeni RP*, „Przegląd Strategiczny" 2014, nr 7, s. 133–141. Pojęcie cyberprzestrzeni najczęściej występuje w zakresie cyberbezpieczeństwa lub cyberprzestępczości, stąd wiele publikacji dotyczy tych zagadnień.

setting up Computer Security Incident Response Teams (CSIRTs) and adopting national cybersecurity strategies. The directive formulates obligations to ensure cybersecurity of the information systems in key service sectors for maintaining critical socio-economic activity, i.e. in energy, transport, banking, financial institutions, the health sector, water supply and digital infrastructure. It introduces the concept of a key service operator, i.e. an entity providing a key service using information systems, in which ICT security incidents could have a significant impact on its provision[9]. The text of the directive focuses on three pillars: institutions that should be established in all Member States, cooperation at the European level, obligations in the area of network and information security. Within the first pillar, each Member State is obliged to establish competent authorities for network and information security, responsible for monitoring the application of its provisions in sectors falling within its scope. Due to the differences in the national governance structures, Member States may designate more than one national competent authority responsible for performing cybersecurity tasks of key service operators and digital service providers[10]. Furthermore, if many competent authorities have been established, each Member State must establish a Single Focal Point to strengthen cooperation between Member States. The Point will collect information about incidents on a national scale and through contact with its counterparts from abroad will strengthen the exchange of information on significant transnational incidents. The last institution required by the directive is CSIRT, covering the entire subject scope of the regulations[11].

The directive left it up to the national legislator to create a system for the operation of public administration authorities to carry out the tasks specified in the Directive. The Act of July 8 on the national cybersecurity system establishes the competent cybersecurity authorities, the Single Contact Point for cybersecurity, and three teams responding to computer security incidents operating at the national level: 1) led by the Minister of National Defence (CSIRT MON); 2) run by the Scientific and Academic Computer Network – the National Research Institute (CSIRT NASK), and 3) run by the Head of the Internal Security Agency (CSIRT GOV)[12].

9 Pkt 31–33 dyrektywy. Zob. także uzasadnienie do projektu…, s. 3–6.
10 Uzasadnienie do projektu…, s. 6.
11 Ibidem.
12 Ibidem.

To begin with, one should present the national cybersecurity system adopted in Poland, listed in an exhaustive list in article 4 of the aforementioned Act to which belong: 1) key services operators; 2) digital services providers; 3) CSIRT MON; 4) NASK CSIRT; 5) CSIRT GOV; 6) sectoral cybersecurity teams; 7) entities of the public finance sector[13]; 8) research institutes; 9) The National Bank of Poland; 10) Bank Gospodarstwa Krajowego; 11) Technical Inspection Office; 12) Polish Air Navigation Agency; 13) Polish Accreditation Centre; 14) National Fund for Environmental Protection and Water Management and voivodship funds for environmental protection and water management; 15) commercial companies carrying out public service tasks; 16) entities providing cybersecurity services; 17) authorities competent for cybersecurity; 18) Single Contact Point for cybersecurity; 19) Government Plenipotentiary for Cybersecurity; 20) Cybersecurity Board.

The specified directory is a closed directory. The government plenipotentiary for cyber security plays a special role in this system whose main task is to coordinate activities and implement the government's policy in the field of cybersecurity[14]. The plenipotentiary is appointed and dismissed by the Prime Minister. The plenipotentiary is the Secretary of State or Under-Secretary of State. Substantive, organisational, legal, technical, office support for the plenipotentiary is provided by the Ministry or other government administration office in which the plenipotentiary has been appointed. Pursuant to the ordinance of the Council of Ministers of March 16, 2018 on the appointment of a government plenipotentiary for cybersecurity, the Secretary of State or Undersecretary of State in the Ministry of National Defence became the plenipotentiary[15]. The plenipotentiary will coordinate tasks and coordinate government policy by means of analysing and assessing the functioning of the national cybersecurity system based on aggregated data and indicators developed with participation of public administration authorities, authorities competent for cybersecurity, CSIRT MON, CSIRT NASK and CSIRT GOV. The plenipotentiary will also supervise the risk management process of the national cybersecurity system using the aggregated data and indicators developed with

13 Ustawa wskazuje, że są to jednostki, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2017 r., poz. 2077 ze zm.).

14 Art. 60 ustawy o krajowym systemie cyberbezpieczeństwa.

15 § 1 ust. 2 rozporządzenia Rady Ministrów z dnia 18 marca 2018 r. w sprawie ustanowienia pełnomocnika rządu do spraw cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 587).

participation of authorities competent for cybersecurity, CSIRT MON, CSIRT NASK and CSIRT GOV.

His tasks in this area will also include giving opinions on government documents, including draft legal acts affecting the implementation of cybersecurity tasks. In his activity, the plenipotentiary should also disseminate new solutions and initiate activities in the area of ensuring cybersecurity at the national level, initiate national cybersecurity exercises and issue recommendations regarding the use of IT devices or software at the request of CSIRT[16]. The plenipotentiary prepares and submits to the Council of Ministers by March 31 each year a report for the previous calendar year containing information on the activities conducted in the area of ensuring cyber security at the national level. Within the scope of its competences, the plenipotentiary may submit to the Council of Ministers proposals and recommendations concerning actions that should be taken by the entities of the national cybersecurity system in order to ensure cybersecurity at the national level and counteract threats in this respect[17].

The Act on the national cybersecurity system also indicates the scope of cooperation of the plenipotentiary with the competent authorities for cybersecurity[18], which concerns cooperation in matters related to

16 Art. 61 ust.1 ustawy o krajowym systemie cyberbezpieczeństwa.

17 Art. 63 ustawy o krajowym systemie cyberbezpieczeństwa. Wskazane rozporządzenie RM także zawiera zadania pełnomocnika rządu do spraw cyberbezpieczeństwa. Należą do nich: 1) analiza i ocena stanu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji rządowej oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego działających w Ministerstwie Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym; 2) opracowywanie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym; 3) opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa; 4) prowadzenie i koordynowanie działań prowadzonych przez organy administracji rządowej mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z internetu; 5) inicjowanie krajowych ćwiczeń z zakresu cyberbezpieczeństwa. Zob. § 2 ust. 2 rozporządzenia Rady Ministrów z dnia 18 marca 2018 r. w sprawie ustanowienia pełnomocnika rządu do spraw cyberbezpieczeństwa.

18 Ustawa w art. 41 wskazała katalog i zakres kompetencji właściwych organów do spraw cyberbezpieczeństwa, którymi są: 1) dla sektora energii – minister właściwy do spraw energii; 2) dla sektora transportu z transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej; 4) dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego; 5) dla sektora ochrony zdrowia z wyłączeniem podmiotów – minister właściwy do spraw zdrowia; 6) dla sektora ochrony zdrowia obejmującego podmioty – minister obrony narodowej;

cybersecurity with other countries, international organizations and institutions, taking activities to support scientific research and development of technologies in the area of cybersecurity, and conducts educational activities aimed at raising public awareness of the threats of cybersecurity and secure use of the internet[19].

The plenipotentiary is also one of the members of the Board at the Council of Ministers, which acts as an opinion-forming and advisory authority in the matters of cybersecurity. The scope of competence of the Board for cybersecurity is indicated in article 65 of the Act on Cyber-security and covers, in principle, expression of opinions on issues concerning directions and plans for counteracting cybersecurity threats, performance by CSIRT MON, CSIRT NASK, the Head of the Internal Security Agency, performing tasks within the framework of CSIRT GOV, sectoral cybersecurity teams and authorities competent for cybersecurity tasks entrusted to them in accordance with directions and plans for counteracting cyber-security threats, as well as expressing opinions in the scope of cooperation between the authorities conducting or supervising CSIRT MON, CSIRT GOV and CSIRT NASK, cooperation between the entities of CSIRT MON, CSIRT NASK, the Head of the Internal Security Agency and the minister – a member of the Council of Ministers responsible for coordinating activities of intelligence services, sector cybersecurity teams and authorities competent for cybersecurity; organization of exchange of information essential for cybersecurity and the international position of the Republic of Poland between government administration authorities and on the conclusions of CSIRT MON, CSIRT NASK or CSIRT GOV regarding recommendations on the use of IT equipment or software. The Board, in addition to the plenipotentiary, includes the Prime Minister as the chairman, secretary of the Board and members of the Board[20].

7) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej; 8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów – minister właściwy do spraw informatyzacji; 9) dla sektora infrastruktury cyfrowej – minister obrony narodowej; 10) dla dostawców usług cyfrowych z wyłączeniem podmiotów – minister właściwy do spraw informatyzacji; 11) dla dostawców usług cyfrowych obejmujących podmioty – minister obrony narodowej.

19 Art. 62 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa.

20 Ustawa o krajowym systemie cyberbezpieczeństwa w art. 66 ust. 1 wskazuje, że członkami Kolegium są: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, minister obrony narodowej, minister właściwy do spraw zagranicznych, szef Kancelarii Prezesa Rady Ministrów, szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez prezydenta Rzeczypospolitej Polskiej, minister – członek Rady

The Act also specified that, in order to coordinate government administration's activities in the scope of cybersecurity, the Prime Minister may, on the basis of the Board's recommendation, issue binding guidelines on ensuring cybersecurity at the national level and the functioning of the national cybersecurity system, as well as request information and opinions in this regard from members of the government[21].

The Minister of Information Technology plays a key role in the process of implementing the provisions of the Act. Based on Article 45 clause 1 of the Act he is responsible for monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland, recommending areas of cooperation with the private sector to increase cybersecurity of the Republic of Poland; preparing annual reports on major incidents reported by key service operators affecting the continuity of their key services in the Republic of Poland and the continuity of their key services in the Member States of the European Union, and significant incidents reported by digital service providers, including incidents involving two or more Member States of the European Union, as well as gathering information on serious incidents that concern or have been forwarded by another Member State of the European Union. The Minister is also responsible for conducting information activities on good practices, educational programmes, campaigns and training to broaden knowledge and build awareness of cybersecurity, including safe use of the internet by various categories of users, and sharing information and good practices related to reporting serious incidents by operators of key services and incidents important by digital service providers. The Minister also, in compliance with Article 46 clause 1 of the Act has competence in the scope of development and maintenance of the ICT system. He also runs a Single Contact Point[22]. The Minister for Information Technology is also responsible for developing, together with the government plenipotentiary, the ministers responsible for the Cyberspace Security Strategy of the Republic of Poland, which the Council of Ministers adopts by resolutions. The strategy takes into account in particular: 1) cybersecurity goals and priorities; 2) entities involved in the

Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – szef Agencji Bezpieczeństwa Wewnętrznego.

21 Art. 67 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa.

22 Art. 48 ustawy o krajowym systemie cyberbezpieczeństwa.

implementation and execution of the strategy; 3) measures to achieve the goals of the strategy; 4) defining measures for readiness, response and restoration of the normal state, including principles for cooperation between the public and private sectors; 5) approach to risk assessment; 6) activities related to cybersecurity educational, informational and training programs; 7) activities related to research and development plans in the area of cybersecurity[23].

The minister in charge of computerisation is obliged to review the provisions of the strategy every two years together with the government's plenipotentiary in charge of cybersecurity.

The Act also distinguishes the tasks of the Minister of National Defence, who is responsible for: cooperation between the Armed Forces of the Republic of Poland and the competent organs of the North Atlantic Treaty Organization, the European Union and international organizations in the area of national defence in the field of cybersecurity, ensuring the capabilities of the Armed Forces of the Republic of Poland in a national, allied and coalition to conduct military operations in the event of a threat to cybersecurity resulting in the need for defence. The Minister is also responsible for developing the skills of the Armed Forces of the Republic of Poland in ensuring cybersecurity by organizing specialized training projects, acquiring and developing tools for building the capacity to ensure cybersecurity in the Armed Forces of the Republic of Poland and assessing the impact of incidents on the state defence system. During martial law, the Minister is responsible for managing incident-related activities and assessing cybersecurity threats, and presenting proposals for defence activities to competent authorities, coordinating – in cooperation with the Minister competent for internal affairs and the Minister competent for computerization – the implementation of tasks of government administration authorities and local government units regarding defence activities in the event of a threat to cybersecurity[24], the Minister of National Defence runs the National Contact Point for cooperation with the North Atlantic Treaty Organizations[25].

The legal solutions presented above have been the subject of numerous consultations and opinions. This fact should be assessed positively, as many aspects that raised reservations were included in the Act. Nevertheless, it is worth looking at these remarks, especially since both government and state

23 Art. 69 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa.
24 Art. 51 ustawy o krajowym systemie cyberbezpieczeństwa.
25 Art. 52 ustawy o krajowym systemie cyberbezpieczeństwa.

administration authorities as well as entrepreneurs and NGOs participated in the consultation process. The Lewiatan Confederation indicated, among others for very broad CSIRT rights in the scope of the possibility to request telecommunications operators to provide information on their activities and the adopted organizational and technical solutions. The introduction of such solutions, in particular bypassing the risk and not taking into account the principle of the adequacy of the security measures used for the identified risks, can significantly reduce the freedom of economic activity and reduce the effectiveness of activities carried out in the field of cybersecurity. Particular attention should be paid to the Confederation's demand on implementing acts, since ordinances have not been subject to consultation, and it is the provisions of implementing acts that will be of significant importance for the entire cyberspace protection system[26]. The National Council of the Judiciary drew attention to the "intersecting subject matter of the draft act" with the applicable Act of April 26, 2007 on crisis management, where the proposed provisions, key services dependent on ICT systems will be subject to the rigors resulting from their inclusion in the uniform list of objects, installations and devices included in the critical infrastructure. For these reasons, the Cybersecurity Act should provide for the mechanisms to control the critical infrastructure protection system resulting from the Crisis Management Act. The Council's doubts were mainly raised by the dualism of regulations regarding the adopted properties of specific ICT systems and services[27]. Therefore, the Minister coordinating special services reported similar comments. Critical infrastructure operators will also be the operators of key services, and this means that they will be forced to report incidents twice.

The minister also expressed concern about the incident reporting system itself, which may be a threat in itself, as it will ultimately contain information on threats that are of key importance to national security[28]. From the point of view of organization and division of competences, the opinion of the

26 Opinia Konfederacji Lewiatan do projektu ustawy o krajowym systemie cyberbezpieczeństwa, online <http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?documentId=0A099FF-19352F4D9C12582B00030CE28>.

27 Opinia Krajowej Rady Sądownictwa do projektu ustawy o krajowym systemie cyberbezpieczeństwa, online <http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?documentId=18D8A80D9E85959AC12582B7004951F6 9>.

28 Opinia ministra koordynatora ds. służb specjalnych do projektu ustawy o krajowym systemie cyberbezpieczeństwa; online<https://legislacja.rcl.gov.pl/docs//2/12304650/12466702/12466705/dokument319798.pdf>.

Minister of National Defence, who issued a negative opinion on the project, was the most interesting. He pointed to the over extensive competences of the Minister for computerisation, at the same time recognizing that it is the Ministry of National Defence that should be the entity that fully exercises military control in the field of cybersecurity[29]. These are just a few remarks received by the Ministry in the process of work on the act. There were so many comments that it is impossible to list all and the entities that participated in the consultations. These remarks were intended to indicate how important and extensive the scope of the regulation is.

The presented scope of tasks and competences of government administration authorities in the scope of cybersecurity does not exhaust the subject in any way. These indications are purely theoretical, as it is too early to assess the practical activity of institutions appointed under the Act and the activities of government administration authorities in the areas of competence that the Act has imposed on them. Implementing these tasks in practice will be of vital importance. First of all, it means creating executive acts that will clarify the operation and mutual relations between public administration authorities and other entities performing tasks in the cyberspace system.

Bibliography

Literature

Berdel-Dudzińska M., *Pojęcie cyberprzestrzeń we współczesnym polskim porządku prawnym*, „Przegląd Prawa Handlowego" 2012, nr 2.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii*, Warszawa 2015.

Skrzypczak J., *Polityka ochrony cyberprzestrzeni RP*, „Przegląd Strategiczny" 2014, nr 7.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Legal acts

Ustawa z dnia 8 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2017 r., poz. 1932). Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2017 r., poz. 1928).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558 ze zm.).

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2017 r., poz. 2077 ze zm.).

Rozporządzenie Rady Ministrów z dnia 18 marca 2018 r. w sprawie ustanowienia pełnomocnika rządu do spraw cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 587).

29 Opinia ministra obrony narodowej do projektu ustawy o krajowym systemie cyberbezpieczeństwa; online <https://legislacja.rcl.gov.pl/docs//2/12304650/12466702/12466705/dokument319646.pdf>.

Polityka ochrony cyberprzestrzeni administracji publicznej na przykładzie organów administracji rządowej wskazanych w ustawie o krajowym systemie cyberbezpieczeństwa

Streszczenie

Konieczność wdrożenia dyrektywy NIS spowodowała zaadaptowanie do polskiego porządku prawnego rozwiązań i pojęć, które uregulują system cyberbezpieczeństwa w cyberprzestrzeni. dyrektywa formułuje obowiązki służące zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, a więc w energetyce, transporcie, bankowości, instytucjach finansowych, sektorze ochrony zdrowia, zaopatrzenia w wodę i infrastrukturze cyfrowej. Ustawa o krajowym systemie cyberbezpieczeństwa wdrażająca dyrektywę wprowadza nowe pojęcie do polskiego porządku prawnego, zatem operatora usługi kluczowej, dostawcy usług cyfrowych, a także określa organy właściwe do spraw cyberbezpieczeństwa, formułując ich zakres zadań i wzajemne relacje.

Słowa kluczowe: krajowy system cyberbezpieczeństwa, pełnomocnik rządu do spraw cyberbezpieczeństwa, administracja rządowa, infrastruktura cyfrowa, usługi cyfrowe, zagrożenie, bezpieczeństwo

Mirosław Karpiuk*

Activities of the local government units in the scope of telecommunication

Abstract

The public sphere which is the closest to the inhabitants is managed by the local government. The legislator entrusted this local government with a number of tasks that should certainly be defined as basic from the point of view of the local and regional communities. These tasks having the nature of a public interest include also tasks related to telecommunication.

The local government units as entities financed to a large extent from the public funds could abuse their market position by competing with telecommunication companies, therefore, they were obliged by the legislator to comply with the rules of the market game, including fair competition. They cannot, therefore, abuse their position in the scope of telecommunication activities or in the case of developing telecommunication infrastructure or sharing it with others.

Key words: local self-government, telecommunication, public utility, telecommunication infrastructure, telecommunication networks, telecommunication entrepreneur, digital services, network operator

* Dr hab. prof. nadzw Mirosław Karpiuk, Wydział Prawa i Administracji, Uniwersytet Warmińsko-Mazurski w Olsztynie, e-mail:miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

Introduction

The local self-government as the basic form of decentralization has been established to meet the needs of residents in the local and regional area. Equipped with appropriate instruments, the coersive apparatus is authorized to perform public tasks passed by the legislator. Due to the principle of independence, the local government activities may be interfered with only in the cases specified by the statutory regulations and only by applying the legality criterion. The attribute of independence allows the local government to implement the adopted policy according to the principles developed by its own authorities, which must, however, comply with the legal regulations.

Territorial self-government is traditionally treated as a manifestation of implementation of the executive power of the state in its functional meaning[1]. Self-government communities are established in principle to exercise public administration, therefore, to implement public tasks within the limits of the constitution and the statutes, with specific (authoritarian) means of action at their disposal[2]. Local government is the form of exercising power in the area that has been located closest to the inhabitants[3]. In the democratic societies, grassroots initiative is very important. Such a grassroot initiative is self-government, including local government, as the structure most involved in the affairs of the local and regional communities and having the broadest competences[4].

Local government participates in the exercise of public authority, and a significant part of public tasks vested in it under the local laws is performed by the self-government on its own behalf and at its own risk[5]. It is a legal entity separate from the state, which is a form of decentralization of the public authority[6].

1 I. Hoffman, J. Fazekas, K. Rozsnyai, *Concentrating or Centralising Public Services? The Changing Roles of the Hungarian Inter-Municipal Associations in the Last Decades*, „Lex localis – Journal of Local Self-Government" 2016, nr 3, s. 454–455.

2 P. Sarnecki [w:] L. Garlicki, M. Zubik (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LEX 2016. J. Kostrubiec, *Samorząd terytorialny* [w:] L. Dubel, J. Kostrubiec, G. Ławnikowicz, Z. Markwart, *Elementy nauki o państwie i polityce*, Warszawa 2011, s. 252.

3 M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014, s. 15.

4 M. Karpiuk, J. Kostrubiec, *Rechtsstatus der territorialen Selbstverwaltung in Polen*, Olsztyn 2017, s. 9.

5 Art. 16 ust. 2 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483 ze zm.).

6 M. Karpiuk, *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym*, Lublin 2008, s. 58.

The scope and operating principles of local government units in the scope of telecommunication

Meeting the community's collective needs is one of the commune's own tasks, which in particular includes matters of telecommunication activities[7]. The administration unit "poviat" performs supra-communal public tasks specified in the acts in the area of telecommunication activities[8]. The voivodship government performs the tasks of a voivodeship character specified by the statutes, in particular, in the scope of telecommunication[9].

In order to meet the collective needs of the self-government community a local government unit may: 1) build or operate telecommunication infrastructure and telecommunication networks and acquire rights to telecommunication infrastructure and telecommunication networks; 2) provide telecommunication networks or provide access to telecommunication infrastructure; 3) provide, by means of the existing telecommunication infrastructure and telecommunication networks, services for: a) telecommunication entrepreneurs, b) special entities, c) end users[10]. As special entities, we should define entities that do not need to have radio licenses, and therefore: 1) organizational units and organizational units subordinate to or supervised by the Minister of National Defence, organizational units and organizational units subordinate to the minister competent for public administration or supervised by him, and organizational bodies and units supervised or subordinate to the minister competent for internal affairs; 2) organizational units and organizational entities subordinate to the minister competent for public administration or supervised by him, organs and organizational units subordinate to the minister competent for internal affairs as well as organizational units of the Internal Security Agency

7 Art. 7 ust. 1 pkt 3a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2019 r., poz. 506 ze zm.), dalej u.s.g. Zobacz także: M. Karpiuk, *Zadania i kompetencje samorządu terytorialnego w czasie stanów nadzwyczajnych* [w:] M. Karpiuk, M. Mazuryk, I. Wieczorek (red.), *Zadania i kompetencje samorządu terytorialnego w zakresie porządku publicznego i bezpieczeństwa obywateli, obronności oraz ochrony przeciwpożarowej i przeciwpowodziowej*, Łódź 2017, s. 99.

8 Art. 4 ust. 1 pkt 23 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz.U. z 2019 r., poz. 511 ze zm.), dalej u.s.p.

9 Art. 14 ust. 1 pkt 15a ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (t.j. Dz.U. z 2019 r., poz. 512 ze zm.), dalej u.s.w.

10 Art. 3 ust. 1 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz.U. z 2017 r., poz. 2062 ze zm.), dalej u.w.r.

in relation to the telecommunication network operated by these bodies and units for the purposes of the President's Office, the Chancellery of the Sejm, the Chancellery of the Senate and government administration; 3) units of the armed forces of foreign states and organizational units of other foreign state bodies, staying temporarily on the territory of the Republic of Poland on the basis of agreements to which the Republic of Poland is a party – for the duration of their stay; 4) organizational units of the Internal Security Agency, Foreign Intelligence Agency and the Central Anti-Corruption Bureau; 5) organizational units subordinate to the minister competent for foreign affairs; 6) diplomatic missions, consular offices, foreign special missions and representations of international organizations, exercising privileges and immunities on the basis of international laws, agreements and customs, having their headquarters in the territory of the Republic of Poland – only to the extent related to the diplomatic activities of these entities; 7) organizational units of the Prison Service; 8) organizational units of the National Tax Administration[11].

Local government activities in the area of telecommunication should comply with Article 3 clause 2 of the Act on supporting the development of telecommunication services and networks, performed: 1) while maintaining compatibility and connectivity with other telecommunication networks created by public entities or financed from the public funds, and while guaranteeing telecommunication undertakings, on the basis of equal treatment, co-use of telecommunication infrastructure and telecommunication networks and access to them; 2) in a transparent and non-distortive manner in the development of equal and effective competition in telecommunication markets. Public utility activities of this nature must not interfere with the competitiveness framework, and thus may not lead to a violation of the market rules, where the local government would have a privileged position over telecommunication companies.

The national regulatory authorities are to support competition in the provision of electronic communications networks and services and associated facilities and services by inter alia: 1) by ensuring that the users, in this the disabled users, are able to draw maximum benefits in respect of variety, prices and quality of the services; 2) by ensuring that there is no distortion or limitation of competition in the electronic communication sector; 3) by

11 Art. 4 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2018 r., poz. 1954 ze zm.), dalej u.p.t.

supporting effective investing in the area of infrastructure and by promoting innovative technologies; 4) by supporting effective use and management of the radio frequencies and numerical resources. The national regulatory authorities are to support the development of the internal market, inter alia: 1) by removing the existing market barriers in the scope of provision of electronic communication networks and services, associated facilities and services, and electronic communications services at the community level; 2) supporting the establishment and development of trans-European networks and the interoperability of pan-European services and end-to-end connectivity; 3) ensuring that in similar circumstances there is no discrimination in the treatment of undertakings providing electronic communications networks and services; 4) cooperating with each other, as well as with the EU Commission, in a transparent manner to ensure consistent application of the law and implementation of the provisions contained in the telecommunication directives. In the pursuit of objectives of the competition support policy, the national regulatory authorities apply objective, transparent, non-discriminatory and proportionate regulatory principles, and in order to do so, they inter alia: (1) promote regulatory predictability by ensuring a consistent regulatory approach in the subsequent review periods; 2) ensure that in similar circumstances there is no discrimination in the treatment of undertakings providing electronic communications networks and services; 3) protect competition for the benefit of consumers and promote, where appropriate, competition based on the infrastructure; 4) promote effective investment and innovation in the new and expanded infrastructure by ensuring that each instance of the obligation to provide access takes into account the risk incurred by the investing enterprises, and by allowing different cooperation agreements between investors and parties requesting access to create investment risk diversification while ensuring market competition and non-discrimination principles; 5) take due account of the conditions related to competition and consumers that occur in different geographical areas in the territory of a given Member State; 6) impose preventive regulatory obligations only in the absence of effective and sustainable competition, and mitigate or waive such obligations as soon as this condition is met[12]. The national regulatory and other competent authorities, as well as the EU Commission and Member States,

12 Art. 8 ust. 2–3 i 5 dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz.Urz. UE L 108, s. 33 ze zm.).

seek to promote competition in the provision of electronic communications networks and associated facilities, including effective infrastructure-based competition as well as in the provision of electronic communications services and the related services[13].

In Article 3 clause 3 of the Act on supporting the development of telecommunication services and networks, the legislator expressly provides that the activity in the area of telecommunications is one of own tasks of a public utility of a local government unit. Therefore, it will be financed from the budget of the local government, because it does not belong to a category of commissioned tasks but to its own.

A local government unit carries out activities in the area of telecommunication on the basis of a resolution of a decision-making body, which follows from Article 3 clause 4 of the Act on supporting the development of telecommunication services and networks. The Legislator of the Act on supporting the development of telecommunication services and networks does not provide for a special majority, therefore resolutions of the commune council, poviat council and voivodship self-government in this matter are adopted by an ordinary majority.

Resolutions of the commune council, as stated in Article 14 clause 1 of the Act on the local government, are passed by an ordinary majority of votes in the presence of at least half of the statutory composition of the council, in an open voting, unless the legislator provides for otherwise. Resolutions on the poviat council and management board, according to Article 13 clause 1 of the Act on the poviat self-government are passed by an ordinary majority of votes in the presence of at least half of the statutory composition of the board, in an open vote, unless provisions of the Act provide for otherwise. The situation is similar in the case of a voivodship governing body, which is confirmed by Article 19 clause 1 of the Act on the voivodeship council. The resolutions of the voivodeship council are passed with a simple majority of votes, in the presence of at least half of the statutory composition of the council, in an open or open roll-call vote, unless the provisions of the Act provide for otherwise.

Article 8 of the Act on supporting the development of telecommunication services and networks provides for the forms of support provided to telecommunication companies in the absence of the possibility of

13 Art. 3 ust. 3 lit. b dyrektywy 2018/1972/UE Parlamentu Europejskiego i Rady z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 321, s. 36–242 ze zm.).

conducting profitable financial activities. A local government unit, entrusting a telecommunication entrepreneur with performance of telecommunication activities, in the case if, due to economic conditions, it is not possible in a given area for a telecommunication entrepreneur to carry out financially profitable telecommunication activities, it may: 1) provide the telecommunication entrepreneur with the infrastructure or telecommunication networks in return for the fees lower than the cost of production; 2) co-finance the costs incurred in providing telecommunication services to end users or telecommunication entrepreneurs for the purposes of providing these services. Such preferences may be used only if it is not possible to carry out profitable financial activities, because otherwise it could distort competition in the telecommunication market.

The local government unit, as the network operator, has an information obligation: 1) under which the President of the Electronic Communications Office may request information on the conditions for providing access to technical infrastructure (imposed by Article 18 clause 2 of the Act on supporting the development of telecommunication services and networks); 2) regarding providing to a telecommunication entrepreneur applying for access to the technical infrastructure with the information related to this infrastructure in the area in which the entrepreneur is planning to implement a fast telecommunication network (imposed by Article 25a clause 1 of the Act on supporting the development of telecommunication services and networks).

As it follows from Article 25c of the Act on supporting the development of telecommunication services and networks, the obligation to provide information by the local government unit being the network operator, and the obligation to enable a telecommunication entrepreneur applying for access to technical infrastructure to inspect specific elements of the technical infrastructure at the place where it is located, does not apply to the technical infrastructure, including critical infrastructure[14], whose use for high-speed telecommunication networks is impossible due to the security and integrity

14 Infrastrukturę krytyczną wymienia art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2019 r., poz. 1398). Zobacz także: M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016, s. 25.

of the technical infrastructure, public health[15], defence[16], state security[17] or

15 W przedmiocie zdrowia publicznego i jego ochrony zobacz szerzej: M. Karpiuk, J. Kostrubiec, *The Voivodeship Governor's Role in Health Safety*, „Studia Iuridica Lublinensia" 2018, nr 2, s. 65–75.

16 W przedmiocie obronności zobacz szerzej: M. Karpiuk, *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019, s. 15–20; M. Bożek, M. Karpiuk, J. Kostrubiec, *Zasady ustroju politycznego państwa*, Poznań 2012, s. 67–70; M. Karpiuk, *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017, s. 21–22; M. Karpiuk, *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1, s. 37–39; J. Kostrubiec, *Zadania i kompetencje samorządu terytorialnego w zakresie administracji rezerw osobowych dla celów powszechnego obowiązku obrony* [w:] M. Karpiuk, M. Mazuryk, I. Wieczorek (red.), *Zadania i kompetencje samorządu terytorialnego w zakresie porządku publicznego i bezpieczeństwa obywateli, obronności oraz ochrony przeciwpożarowej i przeciwpowodziowej*, Łódź 2017, s. 105–106; M. Karpiuk, *Tereny zamknięte ze względu na obronność i bezpieczeństwo państwa ustanawiane przez organy administracji rządowej*, „Ius Novum" 2016, nr 4, s. 196.

17 W przedmiocie bezpieczeństwa zobacz szerzej: M. Czuryk, J. Kostrubiec, *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, nr 1, s. 33–47; M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2, s. 67–70; M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, Bezpieczeństwo państwa. *Zagadnienia prawne i administracyjne*, Olsztyn 2016, s. 17–19; M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3, s. 15; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013, s. 77–89; W. Kitler, M. Czuryk, M. Karpiuk (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013, s. 11–45; M. Karpiuk, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4, s. 10; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018, s. 7; M. Czuryk, *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017, s. 9; M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3, s. 389–390; J. Kostrubiec, *Status of a Voivodship Governor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, nr 5, s. 35–40; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2, s. 227–228; W. Lis, *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej*, Lublin 2015, s. 29–46; K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, s. 15–24; M. Karpiuk, *Zadania administracji publicznej w zakresie bezpieczeństwa społecznego dotyczące wspierania rodziny przeżywającej trudności w wypełnianiu funkcji opiekuńczo-wychowawczych i odnoszące się do systemu pieczy zastępczej*, „Społeczeństwo i Rodzina" 2018, nr 3, s. 54–55; D. Tyrawa, *Gwarancje bezpieczeństwa osobistego w polskim administracyjnym prawie drogowym*, Lublin 2018, s. 40–46; M. Karpiuk, *Pomoc społeczna jako instytucja umożliwiająca rodzinom przezwyciężanie trudnych sytuacji życiowych i jej miejsce w sferze bezpieczeństwa socjalnego*, „Społeczeństwo i Rodzina" 2017, nr 1, s. 41–42; K. Bojarski, *Współdziałanie administracji publicznej z organizacjami pozarządowymi w sferze bezpieczeństwa wewnętrznego w ujęciu administracyjno-prawnym*, Warszawa–Nisko

public safety and order[18]. The legislator sets such values as public health above the information obligation, as well as above the obligation to enable inspection (guaranteed, inter alia, through medical prevention, counteracting and combating epidemics), defence (provided by military means), state security (focused on counteracting threats and removing their effects) or public order (perceived as public and legal order).

A local government unit as a network operator is required to protect classified information[19]. Classified information may be made available only to a person who guarantees confidentiality and only to the extent necessary to perform his/her work or to perform a service in the occupied position or to perform commissioned activities[20]. The local government acting in the area of telecommunication must comply with this rule, otherwise it may threaten or will threaten defence, security, public order or economic interests of a state.

2017, s. 19–72; K. Chałubińska-Jentkiewicz, M. Karpiuk, K. Zalasińska, *Prawo bezpieczeństwa kulturowego*, Siedlce 2016, s. 7.

18 W przedmiocie porządku publicznego zobacz szerzej: M. Karpiuk, K. Prokop, P. Sobczyk, *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017, s. 14–21; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017, s. 96–102, M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9, s. 11.

19 W przedmiocie ochrony informacji niejawnych zobacz szerzej: M. Karpiuk, *Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa*, „Secretum" 2015, nr 2, s. 137–147; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 442–449; M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014, s. 66–75; M. Karpiuk, *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, nr 1, s. 85–99; M. Czuryk, *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017, s. 109–137; M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015, s. 151–173; M. Czuryk, *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015, s. 161–177; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015, s. 33–40.

20 Art. 4 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2019 r., poz. 742). Ustawodawca zawęża dostęp do informacji niejawnych w zakresie podmiotowym – wyłącznie do osób, które dają rękojmię zachowania tajemnicy, czyli tych, które spełniają ustawowe wymogi dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, potwierdzone w wyniku przeprowadzonego postępowania sprawdzającego oraz w zakresie przedmiotowym – do informacji niejawnych, które są niezbędne do wykonywania przez te osoby pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych, I. Stankowska, *Ustawa o ochronie informacji niejawnych. Komentarz*, LEX 2014.

Bibliography

Literature

Bojarski K., *Współdziałanie administracji publicznej z organizacjami pozarządowymi w sferze bezpieczeństwa wewnętrznego w ujęciu administracyjno-prawnym*, Warszawa–Nisko 2017.
Bożek M., Czuryk M., Karpiuk M., Kostrubiec J., *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014.
Bożek M., Karpiuk M., Kostrubiec J., *Zasady ustroju politycznego państwa*, Poznań 2012.
Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.
Chałubińska-Jentkiewicz K., Karpiuk M., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.
Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.
Chałubińska-Jentkiewicz K., Karpiuk M., Zalasińska K., *Prawo bezpieczeństwa kulturowego*, Siedlce 2016.
Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3.
Czuryk M., *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015.
Czuryk M., *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017.
Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.
Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016.
Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016.
Czuryk M., Kostrubiec J., *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, nr 1.
Hoffman I., Fazekas J., Rozsnyai K., *Concentrating or Centralising Public Services? The Changing Roles of the Hungarian Inter-Municipal Associations in the Last Decades*, „Lex localis – Journal of Local Self-Government" 2016, nr 3.
Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4.
Karpiuk M., *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, nr 1.
Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014.
Karpiuk M., *Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa*, „Secretum" 2015, nr 2.
Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.
Karpiuk M., *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1.
Karpiuk M., *Pomoc społeczna jako instytucja umożliwiająca rodzinom przezwyciężanie trudnych sytuacji życiowych i jej miejsce w sferze bezpieczeństwa socjalnego*, „Społeczeństwo i Rodzina" 2017, nr 1.
Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3.
Karpiuk M., *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym*, Lublin 2008.

Karpiuk M., *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017.
Karpiuk M., *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.
Karpiuk M., *Tereny zamknięte ze względu na obronność i bezpieczeństwo państwa ustanawiane przez organy administracji rządowej*, „Ius Novum" 2016, nr 4.
Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2.
Karpiuk M., *Zadania administracji publicznej w zakresie bezpieczeństwa społecznego dotyczące wspierania rodziny przeżywającej trudności w wypełnianiu funkcji opiekuńczo-wychowawczych i odnoszące się do systemu pieczy zastępczej*, „Społeczeństwo i Rodzina" 2018, nr 3.
Karpiuk M., *Zadania i kompetencje samorządu terytorialnego w czasie stanów nadzwyczajnych* [w:] M. Karpiuk, M. Mazuryk, I. Wieczorek (red.), *Zadania i kompetencje samorządu terytorialnego w zakresie porządku publicznego i bezpieczeństwa obywateli, obronności oraz ochrony przeciwpożarowej i przeciwpowodziowej*, Łódź 2017.
Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.
Karpiuk M., Chałubińska-Jentkiewicz K., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.
Karpiuk M., Kostrubiec J., *Rechtsstatus der territorialen Selbstverwaltung in Polen*, Olsztyn 2017.
Karpiuk M., Kostrubiec J., *The Voivodeship Governor's Role in Health Safety*, „Studia Iuridica Lublinensia" 2018, nr 2.
Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.
Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.
Kitler W., Czuryk M., Karpiuk M. (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013.
Kostrubiec J., *Samorząd terytorialny* [w:] L. Dubel, J. Kostrubiec, G. Ławnikowicz, Z. Markwart, *Elementy nauki o państwie i polityce*, Warszawa 2011.
Kostrubiec J., *Status of a Voivodship Governor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, nr 5.
Kostrubiec J., *Zadania i kompetencje samorządu terytorialnego w zakresie administracji rezerw osobowych dla celów powszechnego obowiązku obrony* [w:] M. Karpiuk, M. Mazuryk, I. Wieczorek (red.), *Zadania i kompetencje samorządu terytorialnego w zakresie porządku publicznego i bezpieczeństwa obywateli, obronności oraz ochrony przeciwpożarowej i przeciwpowodziowej*, Łódź 2017.
Lis W., *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej*, Lublin 2015.
Tyrawa D., *Gwarancje bezpieczeństwa osobistego w polskim administracyjnym prawie drogowym*, Lublin 2018.

Legal acts

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483 ze zm.).
Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz.Urz. UE L 108, s. 33 ze zm.).
Dyrektywa 2018/1972/UE Parlamentu Europejskiego i Rady z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 321, s. 36– 242 ze zm.).
Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2018 r., poz. 1954 ze zm.).
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2019 r., poz. 1398).

Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz.U. z 2019 r., poz. 511 ze zm.).
Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (t.j. Dz.U. z 2019 r., poz. 512 ze zm.).
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2019 r., poz. 742).
Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz.U. z 2017 r., poz. 2062 ze zm.).
Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2019 r., poz. 506 ze zm.).

Działalność jednostek samorządu terytorialnego w zakresie telekomunikacji

Streszczenie

Sferą publiczną znajdującą się najbliżej mieszkańców zarządza samorząd terytorialny. Ustawodawca powierzył mu szereg zadań, które z pewnością należy określić jako podstawowe z punktu widzenia lokalnych i regionalnych społeczności. Wśród tego rodzaju zadań, mających charakter użyteczności publicznej, znajduje się również te, które dotyczą telekomunikacji.

Jednostki samorządu terytorialnego jako podmioty finansowane w zdecydowanym zakresie ze środków publicznych mogłyby nadużywać swojej pozycji rynkowej, konkurując z przedsiębiorstwami telekomunikacyjnymi, w związku z czym zostały one przez prawodawcę zobowiązane do przestrzegania reguł gry rynkowej, w tym uczciwej konkurencji. Nie mogą więc one w zakresie działalności telekomunikacyjnej, czy też w przypadku budowy infrastruktury telekomunikacyjnej i jej udostępniania, nadużywać swojej pozycji.

Słowa kluczowe: samorząd terytorialny, telekomunikacja, użyteczność publiczna, infrastruktura telekomunikacyjna, sieci telekomunikacyjne, przedsiębiorca telekomunikacyjny, usługi cyfrowe, operator sieci

Marek Górka*

Działania informacyjne wywiadu w zakresie polityki bezpieczeństwa, w tym w wymiarze cyberprzestrzeni

Streszczenie

Ogromne zmiany i ciągły rozwój zastosowań technologii i komunikacji zmieniły sposób, w jaki postrzegany jest świat. Rewolucja informacyjna miała wpływ na gromadzenie danych wywiadowczych, ich przetwarzanie, analizę i rozpowszechnianie, a także na to, w jaki sposób decydenci mogą uzyskać dostęp do rzetelnych informacji w odpowiednim czasie, a także do źródeł, na których najprawdopodobniej będą polegać, gdy konkretna informacja jest potrzebna do podjęcia decyzji. Niniejszy artykuł próbuje opisać, przeanalizować i wyjaśnić naturę trwającej rewolucji informacyjnej, przedstawić jej główny wpływ na wywiad i politykę bezpieczeństwa oraz omówić znaczenia analizy wywiadowczej w kontekście realizowania działań podczas misji pokojowych.

Słowa kluczowe: polityka bezpieczeństwa, wywiad, kontrwywiad, cyberbezpieczeństwo, misje pokojowe, przetwarzanie informacji, komunikacja, rozwój technologiczny, polityka zagraniczna

* Dr Marek Górka, Wydział Humanistyczny, Politechnika Koszalińska, e-mail: marek_gorka@wp.pl.

Wstęp

Zależność między polityką a wywiadem od dawna uważana jest za kwestię o zasadniczym znaczeniu dla badań w zakresie polityki bezpieczeństwa. Rola służb wywiadowczych jako instytucji pozyskującej dane, jak i tworzącej wiedzę w ramach procesów politycznych nie została jeszcze szczegółowo przedyskutowana na forum akademickim. Wynika to przede wszystkim z poufnego charakteru informacji, który stanowi często podstawową barierę w budowaniu wiedzy na temat funkcjonowania tajnych służb. Drugim kluczowym problemem jest dynamicznie zmieniająca się rzeczywistość polityczno-gospodarcza, która sprawia, że trudno jest przewidzieć przyczyny, jak i konsekwencje określonych wydarzeń. Nie bez znaczenia jest także rewolucja technologiczna, która poprzez cyberprzestrzeń utworzyła alternatywną sferę rywalizacji międzynarodowej. Ponadto nowe narzędzia cyberkomunikacji sprawiły, że dotychczas znane zjawiska jak dezinformacja czy też wojna informacyjna nabrały nowego znaczenia dla politycznego otoczenia.

Przyczyną podjęcia się zagadnień związanych z wywiadem stały się pytania, które często pojawiają się w przestrzeni publicznej i dotyczą skuteczności tajnych służb w walce ze współczesnymi zagrożeniami. Obraz ewolucyjnego charakteru prowadzenia tajnych działań prowokuje także do refleksji o to, czy obecnie dominującą rolę odgrywają jeszcze ludzie, czy też metody i technologia? Innymi słowy, postęp technologiczny sprawia, że w działalności wywiadowczej może być zachwiana równowaga pomiędzy potencjałem ludzkim i potencjałem technicznym. Jednak to tylko człowiek widzi pewne zależności i podobieństwa między danymi, zjawiskami czy też wydarzeniami. I to właśnie on z pojedynczych elementów – jak puzzle – tworzy obraz zachodzących procesów i zjawisk. Bez odpowiedniej informacji, która daje możliwość realnego obrazu sytuacji, wszelkie podejmowane operacje będą działaniami na oślep, na skutek których ucierpią prawa i wolności obywatelskie.

Celem pracy jest udzielenie odpowiedzi na pytanie dlaczego i w jaki sposób wywiad może mieć wpływ na politykę zagraniczną państwa? Czym jest wywiad i jaką spełnia rolę w obronności państwa? W jaki sposób informacja wywiadowcza jest przydatna dla sił zbrojnych, szczególnie podczas wykonywania misji pokojowych? Na ile cyberprzestrzeń jest domeną technologii i biznesu, a na ile państwa, które wyznacza i realizuje politykę bezpieczeństwa? Jak wytyczyć granice między wolnością a bezpieczeństwem oraz ile wolności można poświęcić w kontekście współczesnych zagrożeń? Praca ma także za zadanie wskazać najważniejsze wyzwania dla służb wywiadowczych we współczesnej

polityce bezpieczeństwa. Czynnik ten jest kluczowym problemem w kształtowaniu decyzji przez decydentów politycznych. Okazuje się bowiem, że zdefiniowanie roli i znaczenia służb w przestrzeni politycznej definiuje również stosunek władz do dwóch ścierających się wzajemnie wartości, jakimi są wolność i bezpieczeństwo.

Aby odpowiedzieć na powyższe pytania warto odnotować stan badań w polskiej literaturze przedmiotu[1]. Poszczególne prace przynoszą – w większości przypadków – odpowiedź na złożone w swej naturze zjawiska. Wartościowym uzupełnieniem są oczywiście artykuły naukowe[2] oraz publicystyczne, które tworzone są na podstawie trudno dostępnych źródeł, dzięki czemu wypełniają one lukę w dotychczasowej wiedzy w zakresie służb wywiadowczych. Ważnym elementem w pracy jest pojęcie informacji, które definiowane jest w artykule w kontekście zarówno cyberprzestrzeni, zagrożeń terrorystycznych, misji pokojowych, jak i poszczególnych elementów bezpieczeństwa składających się na wewnętrzną politykę państwa.

Służby wywiadowcze jako wyzwanie badawcze – wybrane aspekty

Wywiad jest działalnością państwa, która realizowana jest w ukryciu. Tajność tej instytucji jest zarazem największą barierą jeśli chodzi o analizę tego typu służby. Teoretycy w swoich badaniach zazwyczaj dochodzą do pewnego

1 Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009; W. Wróblewski (red.), *Wywiad i kontrwywiad w świecie*, Szczecin 2009; M. Minkina, *Wywiad Federacji Rosyjskiej*, Siedlce 2012; L. Pawlikowicz, *Aparat centralny 1 Zarządu Głównego KGB jako instrument realizacji globalnej strategii Kremla 1954–1991*, Warszawa 2013; M. Minkina, *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Warszawa 2014; A. Gruszczak, *Europejska wspólnota wywiadowcza. Prawo – instytucje – mechanizmy*, Kraków 2014; M. Minkina, B. Gałek, *Gry wywiadów. Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015; M. Górka, *Mossad. Porażki i sukcesy tajnych służb izraelskich*, Warszawa 2015; M. Minkina, *FSB. Gwardia Kremla*, Warszawa 2016; M. Berliński, R. Zulczyk, *Federalna Służba Bezpieczeństwa Federacji Rosyjskiej*, Warszawa 2016; M. Górka (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa 2016; M. Górka (red.), *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa: historia i współczesność*, Toruń 2016; J. Larecki, *Wielki leksykon tajnych służb specjalnych świata*, Warszawa 2017; A. Bielska, P. Smółka (red.), *Wywiad biznesowy*, Piaseczno 2017.

2 Na szczególną uwagę zasługuje czasopismo naukowe „Secretum. Służby specjalne. Bezpieczeństwo. Informacja" oraz „Studia Politologiczne" z 2018 r. z numerem 43, które w całości poświęcony jest Służbom specjalnym w państwach poradzieckich.

momentu, który już dalej nie pozwala na wiarygodny i rzeczywisty opis działalności służb. Z kolei praktycy, nawet będący w stanie spoczynku i posiadający szeroką wiedzę, nie mogą wiele ujawnić z powodu obowiązującej ich w dalszym ciągu tajemnicy państwowej. A zatem pozostaje niezagospodarowana przestrzeń, z wieloma niedopowiedzeniami, które tworzą wyobrażenia i domysły. W ten sposób powstają mity na temat tajemniczego, sensacyjnego i na wpół romantycznego świata służb wywiadowczych. Wymownym tego przykładem jest Mossad. Agencja ta nie posiada rzecznika prasowego, a zatem nie ma ona potrzeby komentować czegokolwiek czy też prostować lub wyjaśniać. Tym samym pozostawia ona szeroką przestrzeń dla domysłów, które w pewien sposób tworzą wizerunek wszechpotężnej służby[3].

Wokół wywiadu narosło wiele legend, nie każda z nich jednak jest prawdziwa, podobnie jak z filmami akcji. Okazuje się, że wywiad znacznie odbiega od potocznych wyobrażeń. Jego zadaniem jest m.in. zdobywanie danych i budowanie na ich podstawie wartościowych informacji dla władz. A zatem kwintesencją tej specjalności jest wiedza, która daje przewagę nad przeciwnikiem. Nie bez powodu w języku angielskim wywiad nosi nazwę „intelligence"[4]. Częstym przymiotnikiem występującym podczas określania służb jest słowo „specjalne" albo też „tajne". Można powiedzieć, że służby to normalne instytucje państwowe, które pracują w obszarze nie do końca stabilnym i bezpiecznym. One jako pierwsze posiadają informacje o zagrożeniu dla państwa i jego obywateli, ale też jako pierwsze nawiązując i/lub podtrzymują kontakty między zwaśnionymi stronami. I tak jak w dyplomacji, tak też w wywiadzie nie ma na stałe sojuszników ani wrogów.

Tak zaistniały model rywalizacji wywiadowczej wynika po pierwsze: z sytuacji, w której dzisiejszy przeciwnik może jutro być partnerem do współpracy i odwrotnie obecny sojusznik może jutro być konkurentem, dlatego tak ważna w tej służbie jest tajemnica. Ponadto świat wywiadu to sieć wzajemnie krzyżujących się interesów. Po drugie: nawet zaprzyjaźnione służby wywiadowcze zbierają informację na temat swoich sojuszników. Bardzo dobrym tego przykładem są relacje wywiadowcze pomiędzy USA a Izraelem. Oba państwa

3 P. Tyler, *Twierdza Izrael. Zakulisowa historia elit wojskowych, które uparcie bronią się przed pokojem*, Poznań 2014, s. 13–14; Y. Melman, *Mossad'ssplitpersonality*, „The Jerusalem Report" z dnia 31 grudnia 2012 r., s. 34; G. Shimron, *The Mossad and the Myth*, Tel Awiw 1996, s. 101.

4 M. Minkina, *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, s. 28.

współpracują ze sobą i uznają, że nie będą podejmować działań wywiadowczych na terytorium sojusznika. Jednak żadna ze stron nie dotrzymuje tej „niepisanej" umowy[5].

Zadaniem wywiadu jest więc ocena i diagnoza drugiej strony, na ile ona jest sojusznikiem a na ile przeciwnikiem. Wywiad działa więc na zasadzie ukrytej dyplomacji. Służby pozyskują źródła informacji, które pozwalają im na minimalizowanie niepewności w świecie wysoko niestabilnym. Wywiad to także organizacja odgrywająca pierwszą rolę w rywalizacji między państwami. I to on podobnie jak dyplomacja funkcjonuje poza granicami własnego państwa, często bez zgody władz kraju, na terytorium którego działa[6]. A zatem w pewien sposób jest nielegalny. Wywiad to organizacja, która może działać na poziomie zarówno politycznym, militarnym, jak i gospodarczym. Może to być narzędzie państwa, jak i korporacji. Sektor publiczny współcześnie przejmuje wiele funkcji państwa, odpowiada za funkcjonowanie infrastruktury krytycznej, dlatego też jest istotny z punktu widzenia bezpieczeństwa państwa. Ponadto wchodząc w współpracę z państwem, korporacje nabywają wiele informacji o charakterze tajnym. Obecnie lub w niedalekiej przyszłości wywiad skazany będzie na współpracę z sektorem publicznym. Następuje zatem zacieranie granic nie tylko semantycznych pomiędzy wywiadem i kontrwywiadem, które mają inny obszar działania, ale i również pomiędzy formułą instytucji państwowych i organizacji prywatnych.

Kolejnym wyzwaniem badawczym pojawiającym się przy opisie pracy służb wywiadowczych – zasygnalizowanym już na wstępie artykułu – jest wyznaczenie granicy między wolnością a bezpieczeństwem. Opozycja tych dwóch wartości okazuje się często problemem nie do rozwiązania. W walce z terroryzmem wszystkie te wartości ulegają awarii lub paraliżowi. Nie można mieć 100% bezpieczeństwa i 100% prywatności. Charakterystyczne jest zjawisko, że najwięcej krytyki, co do formy monitorowania oraz inwigilacji obywateli przez służby, mają te osoby, które okazują się największymi ekshibicjonistami na portalach społecznościowych[7].

5 E. Kahana, *Mossad – CIA Cooperation*, „International Journal of Intelligence and CounterIntelligence" 2001, nr 14, s. 410.

6 M. Górka, *Dyplomacja i wywiad. Przyczynek do refleksji nad polityką bezpieczeństwa* [w:] M. Górka (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa 2016, s. 64–82.

7 M. Górka, *Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 r.*, „e-Politikon" 2017, nr 19, s. 49–79.

Działań w cyberprzestrzeni nie można rozpatrywać w oderwaniu od działań wywiadowczych, czy też zagrożeń dotyczących bezpieczeństwa cybernetycznego w danym państwie. W tym celu agencje wywiadowcze przyjęły proaktywne stanowisko wobec środowisk akademickich, biznesowych i obywatelskich oraz ustanowiły ramy współpracy, które pozwoliłyby im wszystkim zapewnić ochronę i bezpieczeństwo swojej pracy.

Analiza wywiadowcza

Wiele analiz wywiadowczych potwierdza i uzupełnia wiedzę środowisk politycznych, co może w potocznym rozumieniu prowadzić do błędnych wniosków, że praca analityków wywiadu jest zbędna. Jak bardzo jest to mylne przekonanie, świadczy szybki postęp technologiczny, który doprowadził do powstania instrumentów, zmieniających proces dostępu do informacji, umożliwiając użytkownikom niemal natychmiastowy wgląd do danych na całym świecie. Dlatego w erze informacyjnej, charakteryzującej się przepełnieniem treści, głównym wyzwaniem nie jest już pozyskiwanie danych, ale identyfikacja istotnych informacji i powiązanie ich z wcześniej określoną wiedzą. A zatem wywiad więcej pozyskuje danych niż może przeanalizować, dlatego też istnieje potrzeba dokonywania selekcji treści, czasem także ich ignorowania, co może być przyczyną późniejszej tragedii, czego przykładem jest niespodziewany atak, który dał początek wojnie YomKippur w 1973 r. czy też symboliczny już zamach z 11 września 2011 r.[8]

Celem analizy wywiadowczej jest zapewnienie wsparcia organom decyzyjnym, a jednym z głównych wymogów skutecznego działania jest zmniejszenie subiektywności przekazywanych informacji, tak aby były one jak najbardziej zbliżone do rzeczywistości. Dlatego tak ważne jest w pracy wywiadu krytyczne myślenie oraz kreatywne rozwiązywanie problemów.

Postęp technologiczny wpłynął również na analizę wywiadu, bowiem w znaczny sposób zróżnicował on środowisko informacyjne. Pojawiło się znacznie więcej źródeł informacji, z których każde ma inny stopień wiarygodności, co może powodować, że informacje będą niekompletne, sprzeczne lub niespójne. Informacje o nieokreślonej wiarygodności są charakterystyczne dla

8 E. Stephens, *Caught on the hop: the Yom Kippur war*, „History Today" 2008, vol. 58/10, s. 44–50.

działań wywiadowczych, a zatem są warunkiem koniecznym do ich skutecznej oceny, nawet w przypadku, gdy obraz określonych wydarzeń nie jest kompletny[9].

Obecnie zasady wywiadu są przyjmowane i stosowane nie tylko na szczeblu politycznym i wojskowym, ale również na szczeblu gospodarczym i społecznym, gdzie potrzebna jest strategia. Wywiad obejmuje gromadzenie, przetwarzanie, analizę i rozpowszechnianie informacji wywiadowczych potrzebnych do opracowania i wdrożenia strategii, a zatem polityki i planów na poziomie krajowym, regionalnym i międzynarodowym.

Pierwszym krokiem do opracowania strategii bezpieczeństwa narodowego jest analiza strategiczna środowiska (krajowego i międzynarodowego), w którym działa państwo, identyfikacja głównych zagrożeń i szans związanych z interesem narodowym. Drugim krokiem jest opracowanie i wybór celów, po którym następuje opcja odpowiednich kierunków działania niezbędnych do osiągnięcia celów. Zasadniczo strategia musi być zgodna z interesem narodowym państwa na podstawie jego instrumentów władzy. W wyniku zaangażowania decydentów w opracowywanie i wdrażanie strategii zakłada się, że przedstawiciele obywateli będą dbać o dobro państwa na wszystkich szczeblach: politycznym, gospodarczym, wojskowym, społecznym, kulturalnym i środowiskowym. Ponadto decydenci strategiczni muszą mieć dokładny obraz międzynarodowego środowiska strategicznego oraz ryzyka, zagrożeń i możliwości, a także kosztów związanych z wyborem określonego sposobu działania. W tym celu elity polityczne potrzebują wiedzy, a wywiad może ją dostarczyć. Służby mogą przekazywać nie tylko fakty, ale również, przy wsparciu działań wywiadowczych, gromadzić dane, które są przetwarzane, a uzyskane w jego wyniku informacje przekazywać odpowiednim organom lub analitykom wywiadu do ponownego wykorzystania[10]. I to oni muszą zweryfikować integralność i prawidłowość zgromadzonych danych, wybierając i wykorzystując nowe wybrane informacje w celu opracowania trwałych danych wywiadowczych przedstawiających środowisko strategiczne i zapewniających oceny na przyszłość[11].

9 T. Mattern, J. Felker, R. Borum, G. Bamford, *Operational Levels of Cyber Intelligence*, „International Journal of Intelligence and CounterIntelligence" 2014, vol. 27/4, s. 702–719.
10 W.J. Lahneman, *The Need for a New Intelligence Paradigm*, „International Journal of Intelligence and Counterintelligence" 2010, vol. 23/2, s. 209.
11 R. Omilianowicz, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej* [w:] W. Wróblewski, *Wywiad i kontrwywiad w świecie*, Szczecin 2009, s. 145–158.

Gromadzenie, analizowanie i rozpowszechnianie trwałych danych wywiadowczych do wykorzystania przez politycznych decydentów oznacza w rzeczywistości, że narzędzie do przewidywania różnych kierunków działań jest dostarczane poprzez identyfikację kluczowych punktów innych regionalnych lub międzynarodowych podmiotów. W związku z tym można zidentyfikować główne tendencje i czynniki, które prowadzą do określonej sytuacji strategicznej. W tym cyklu wywiadowczym kluczowym elementem całego procesu jest faza analizy, w związku z czym analityk odgrywa kluczową rolę w powodzeniu tego procesu, ponieważ wnosi wiedzę fachową i ramy analityczne niezbędne do wyjaśnienia perspektywy strategicznej, na podstawie której podejmuje się decyzje. Analitycy wnoszą wkład na każdym etapie procesu decyzyjnego, począwszy od właściwego zdefiniowania interesów państwowych, a skończywszy na celach i kierunkach działań[12]. Analityk wywiadu zapewnia ocenę reakcji otoczenia po wprowadzeniu i realizacji przygotowanych działań, pozwalając w ten sposób decydentom na wybór najlepszego rozwiązania w danym przedziale czasowym. Mając na uwadze rolę analityka w opisywanym powyżej procesie, można stwierdzić, że wywiad nie ogranicza się do pierwszego etapu rozwoju strategii, czyli analizy strategicznej, ale koncentruje się na ciągłym, dogłębnym procesie wspierania sformułowanej strategii państwa.

Cyberprzestrzeń jako wymiar polityki bezpieczeństwa

Debata na temat cyberbezpieczeństwa nie powinna być tylko prowadzona z perspektywy, technologicznej. Do pełnego zrozumienia cyberzagrożeń konieczna jest opinia prawników, socjologów, politologów w celu wyjaśnień wielu krzyżujących się procesów zarówno w skali lokalnej, jak i globalnej. Aby więc zredukować zagrożenia do najniżej możliwego poziomu, potrzebna jest świadomość, że o stopniu poczucia cyberbezpieczeństwa nie stanowi tylko technologia, ale i ludzkie motywacje oraz zachowania.

Cyfrowa rewolucja ma wpływ na funkcjonowanie większości rządów na świecie oraz na bezpieczeństwo przedsiębiorstw i obywateli. Trudność jednak w analizie tych procesów polega na ich bardzo dynamicznej i złożonej naturze. Wczorajsze technologie oraz aplikacje są dziś – jak często się okazuje – już nie

12 M. Degaut, *Spies and Policymakers: Intelligence in the Information Age*, „Intelligence and National Security" 2016, vol. 31/4, s. 509–531.

aktualne i nieadekwatne do potrzeb ich użytkowników. Dużą rolę spełnia tu nauka, której zadaniem jest wyjaśnienie i zrozumienie zachodzących procesów. Ta perspektywa pozwala łączyć analizę ryzyka w cyberprzestrzeni z dyscyplinami humanistycznymi.

Cyberataki mogą pochodzić z dowolnego miejsca na świecie, bez ponoszenia dużych kosztów po stronie atakujących. Jest to z pewnością największe wyzwanie dla bezpieczeństwa i stabilności instytucji wykonywujących zadania w strategicznym obszarze państwa. Jednak przedsiębiorstwa lub osoby będące ofiarą cyberataku zwykle nie udzielają informacji na ten temat, a zatem profilaktyka w zakresie cyberbezpieczeństwa jest utrudniona. Ważną rolę w tej sytuacji spełniają służby wywiadowcze i kontrwywiadowcze, które z jednej strony poprzez swą specjalizację udzielają pomocy, a z drugiej strony w sposób poufny – czyli bez informowania opinii publicznej – są w stanie podjąć określone działania. Obecnie zdecydowana większość organizacji ulega – bądź może ulec – zagrożeniom płynącym ze strony podmiotów funkcjonujących w cyberprzestrzeni[13].

Okazuje się, że nawet demokratyczne reguły wyborcze w wielu państwach mogą być naruszone w wyniku dezinformacji, jaka ma miejsce w cyberprzestrzeni. Kampania prezydencka w USA w 2016 r. jest tego przykładem. Śledztwo prowadzone przez stronę amerykańską ujawniło zastosowanie cybertechnologii w celu podejmowania wysiłków obcych służb wywiadowczych mających wpłynąć na wewnętrzną politykę innego państwa. Kolejne zeznania złożone w 2017 r. przez kilku urzędników amerykańskich, w szczególności przez byłego dyrektora FBI Jamesa Comeya oraz dyrektora NSA Admiral Mike Rogers, potwierdziły wcześniejsze podejrzenia, że Rosja za pomocą swoich służb podejmowała próby ingerencji w wybory w USA w nadziei na ukształtowanie wyników głosowania zgodnie z własnymi celami[14]. Ponadto stwierdzono, że Rosja, korzystała m.in. z programów komputerowych tzw. „botów", które imitują ludzkie zachowania[15]. Dzięki właśnie tym narzędziom, próbowano poprzez m.in. dezinformację rozpowszechniać fałszywe treści, które następnie miały wpływać na zachowania wyborcze. Według badań Uniwersyte-

13 M. Rudner, *Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge*, „International Journal of Intelligence and CounterIntelligence" 2013, vol. 26/3, s. 453–481.
14 A. Wilner, *Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation*, „Comparative Strategy" 2017, vol. 36/4, s. 309–318.
15 L. Barber, *Fake news in the post-factual age*, „Financial Times" z dnia 16 września 2017, https://www.ft.com/content/c8c749e0-996d-11e7-b83c-9588e51488a0.

tu Oxfordzkiego prawie jedna czwarta treści internetowych udostępnianych na Twitterze przez użytkowników w stanie Michigan, podczas ostatnich dni kampanii wyborczej w USA, stanowiła tzw. „fake newsy". W opublikowanym raporcie stwierdza się ponadto, że fałszywe wiadomości stanowiły 23% treści domen internetowych. Rozpowszechnianie fałszywych wiadomości, w szczególności za pośrednictwem mediów społecznościowych, może okazać się kluczowe dla sposobu postrzegania debaty politycznej[16]. A jeśli jeszcze bierze się pod uwagę, iż około 62% dorosłych Amerykanów ma dostęp do wiadomości m.in. poprzez portale społecznościowe, to można sądzić, że każda informacja zamieszczona w cyberprzestrzeni może wywołać ogromny rezonans społeczny[17]. Wzrastająca liczba użytkowników internetu zauważalna jest także w państwach europejskich i może stanowić dowód potwierdzający zjawisko uzależnienia społecznego od technologii.

Tabela. Liczba użytkowników internetu w państwach Unii Europejskiej w 2016 r.[18]

2016 rok			
Państwo UE	Użytkownicy internetu	Stosunek użytkowników internetu do ogółu populacji	Populacja państwa
Austria	6,953,400	81.1%	8,569,633
Belgia	10,060,745	88.5%	11,371,928
Bułgaria	4,155,050	58.5%	7,097,796
Chorwacja	3,133,485	74.2%	4,225,001
Cypr	844,680	71.8%	1,176,598
Czechy	9,323,428	88.4%	10,548,058
Dania	5,479,054	96.3%	5,690,750
Estonia	1,196,521	91.4%	1,309,104
Finlandia	5,107,402	92.5%	5,523,904
Francja	55,860,330	86.4%	64,668,129
Grecja	7,072,534	64.8%	10,919,459
Hiszpania	37,865,104	82.2%	46,064,604
Holandia	15,915,076	93.7%	16,979,729
Irlandia	3,817,392	81%	4,713,993
Litwa	2,199,938	77.2%	2,850,030
Luksemburg	548,807	95.2%	576,243

16 D. Blood, *Fake news is shared as widely as the real thing*, „Financial Times" z dnia 27 marca 2017, https://www.ft.com/content/99ea2fae-107c-11e7-b030-768954394623,
17 L. Barber, *Fake…*, op. cit.
18 Obliczenia własne na podstawie, za: http://www.internetlivestats.com/internet-users-by-country.

2016 rok			
Państwo UE	Użytkownicy internetu	Stosunek użytkowników internetu do ogółu populacji	Populacja państwa
Łotwa	1,491,951	76.3%	1,955,742
Malta	334,056	79.6%	419,615
Niemcy	71,016,605	88%	80,682,351
Polska	27,922,152	72.4%	38,593,161
Portugalia	6,930,762	67.3%	10,304,434
Rumunia	11,236,186	58%	19,372,734
Słowacja	4,477,641	82.5%	5,429,418
Słowenia	1,490,358	72%	2,069,362
Szwecja	9,169,705	93.1%	9,851,852
Węgry	7,874,733	80.2%	9,821,318
Wielka Brytania	60,273,385	92.6%	65,111,143
Włochy	39,211,518	65.6%	59,801,004

Zgodnie z powyższymi danymi, okazuje się, że wśród państw tzw. „nowej Europy", (lub inaczej państw postkomunistycznych), średnia użytkowników internetu wynosi 77,28%. Natomiast jeśli chodzi o państwa tzw. „starej Europy", czyli te o znacznie dłuższym doświadczeniu w funkcjonowaniu w warunkach gospodarki liberalnej, średnia ta jest wyższa i wynosi 82,71%. Różnica ta wynika – jak już zasygnalizowano – z posiadania znacznie zaawansowanych zasobów technologicznych przez gospodarkę danego państwa, a także wyższy poziom rozwoju naukowego oraz innowacyjności. A czynniki te, jak można sądzić, są m.in. pokłosiem wielu lat funkcjonowania tych państw w rzeczywistości gospodarki wolnorynkowej. Paradoksalnie jednak większy rozwój cybertechnologii nie musi oznaczać wzrostu poziomu cyberbezpieczeństwa, bowiem dotychczasowe, analogowe systemy odpowiedzialne za m.in. pracę infrastruktury krytycznej, są znacznie bardziej odporne na jakiekolwiek cyberincydenty.

Każdego dnia coraz częściej społeczeństwo, w wyniku wielu cyber udogodnień, staje się uzależnione w wielu dziedzinach życia od urządzeń elektronicznych. Jednak budowanie przyszłości w oparciu o cybertechnologię, którą coraz trudniej jest chronić i kontrolować, może skutkować wieloma zagrożeniami. Globalna ekspansja sieci społecznościowych (takich jak Facebook, Twitter) wraz z rosnącą komunikacją sieciową może doprowadzić do tego, że cybertechnologia wymknie się spod kontroli. Już dziś wiele informacji, błędnie zinterpretowanych lub umyślnie fałszowanych, żyje swoim życiem i tworzy fikcyjną rzeczywistość.

Istnieją realne obawy, że cyberprzestępcy będą blokować nie tylko komputery, ale i pozostałe urządzenia podłączone do internetu, z których na co dzień społeczeństwo korzysta. Awarii mogą więc ulec, np. telefony, telewizory, zegarki, urządzenia medyczne, opaski sportowe czy też choćby aparaty służące do pomiaru glukozy. Celem paraliżu tego typu systemów jest m.in. wyłudzenie okupu od właścicieli tychże urządzeń. Ostatnie cyberataki zaistniałe przy pomocy złośliwego oprogramowania typu ransomware jak „WannaCry" i „Petya" stanowią doskonałą ilustrację tego, jakie skutki mogą one przynieść[19].

Ataki na strony internetowe poważnych instytucji politycznych, gospodarczych są dowodem na to, że nikt nie jest odporny na działania hakerów, które są coraz bardziej wyrafinowane. Administracja publiczna, systemy finansowe, centralne sieci energetyczne zawsze były celem hakerów ze względu po pierwsze na wartość informacji, jakie te instytucje posiadają, a po drugie ze względu na rozmiar konsekwencji, które mogą zaistnieć na skutek zastosowania złośliwego oprogramowania. Patrząc w niedaleką przyszłość można sądzić, że zagrożenia bezpieczeństwa komputerowego będą dominować na tle dzisiejszych zagrożeń gospodarczych i społecznych.

Kradzież danych z karty kredytowej lub z innych dokumentów osobistych oraz oszustwa bankowe, masowy spam oraz szantaż, to tylko kilka przykładów, które świadczą o tym, jak szerokie spektrum przestępstw oferuje cyberprzestrzeń. Każde z urządzeń podłączonych do internetu jest okazją do włamania. Cyberatak jest stosunkowo prostą czynnością, bo nie ma doskonałych programów. Jednak dla skutecznego uzyskania danych nie zawsze konieczny jest cyberatak. Zazwyczaj wymaga to połączenia dwóch czynników: podatności technicznych oraz innego człowieka, którego frustracja, brak motywacji lub też nadmierne zaufanie (połączona z naiwnością) prowadzi do współudziału umożliwiającego dostęp do poufnych informacji. Obecnie, gdy coraz więcej instytucji zapewnia większy dostęp online swoim klientom, profesjonalni przestępcy z powodzeniem wykorzystują techniki phishingowe w celu kradzieży danych umożliwiających podszywanie się pod dowolną osobę lub bezpośrednie pozyskiwanie w nielegalny sposób środków finansowych.

Większość metod fałszowania wykorzystuje określoną formę oszustwa technicznego, która ma na celu utworzenie łącza w e-mailu oraz sfałszowanej – ale łudząco podobnej – strony internetowej, która prowadzi ofiarę do

19 W. Fripp, *The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age*, „Intelligence and National Security" 2018, vol. 33/4, s. 623–626.

fałszywej organizacji. Ten rodzaj kradzieży staje się coraz popularniejszy ze względu na łatwość, z jaką nie podejrzewający ludzie często ujawniają osobiste informacje oszustom, w tym numery kart kredytowych, numery ubezpieczenia społecznego, imiona członków rodziny itp. Istnieje również realna możliwość, że złodzieje tożsamości mogą pozyskiwać informacje poprzez dostęp do rejestrów publicznych. Po uzyskaniu tych informacji oszuści mogą używać danych osobowych do tworzenia fałszywych kont w imieniu ofiary, czy też uniemożliwiać ofiarom dostęp do własnych kont.

Popularną metodą jest także wysyłanie e-maili, które ostrzegają użytkownika, z niewielkim lub nieznacznym wyprzedzeniem, że konto zostanie zamknięte, dopóki osoba będąca właścicielem konta nie potwierdzi ponownie danych wymaganych przy operacjach finansowych. Do częstych przypadków można zaliczyć także otrzymywanie wiadomości na pocztę elektroniczną z dołączonymi formularzami zgłoszeniowymi. Tego typu informacje są zazwyczaj opatrzone uzasadnionym i wiarygodnym komunikatem, tylko po to, by przekonać ofiarę do udostępnienia danych do konta[20]. Innymi słowy: każdy przestępca, który spędza trochę czasu przed ekranem monitora może pozyskać bogatą wiedzę o każdej, wybranej osobie. Może on wykorzystać te informacje, aby spreparować wiarygodną wiadomość, która w zamierzeniu oszusta ma pochodzić od nadawcy np. członka rodziny, przyjaciela lub kolegi, którego darzymy zaufaniem, w celu wyłudzenia danych, a za ich pomocą naszych pieniędzy.

Wywiad gospodarczy

Zakres narzędzi socjotechnicznych jest ogromny, ponieważ można tworzyć fałszywe tożsamości i budować zaufanie bez dokonywania fizycznych włamań. I nie chodzi tu o atakowanie komputerów, bo stanowią one jedynie narzędzie, ostatecznym celem są zawsze ludzie. Informacje, które są zbierane przez aplikacje ze wszystkich sieci społecznych, zarówno w kontekście indywidualnym, jak i zbiorowym (czyli rodzina, przyjaciele, współpracownicy ofiary), są nieocenionym źródłem w rękach oszustów, ponieważ mogą oni dostosowywać atak do konkretnej osoby.

20 M. Górka, *Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa*, „Systemy wspomagania inżynierii produkcji" 2017, vol. 6/5, s. 73–89.

Obecnie wiele organizacji w sektorze prywatnym działa w analogiczny sposób jak wywiad. Informacje, bardziej niż kiedykolwiek, dają władzę, która umożliwia kradzież jeszcze cenniejszych danych niż dane osobowe. Daje zatem możliwość pozyskania najlepiej strzeżonych tajemnic instytucji państwowej bądź korporacji. Zrozumienie tego zjawiska ma fundamentalne znaczenie dla wyjaśnienia, dlaczego firma powinna bardziej niż kiedykolwiek zwracać uwagę na poufność danych własnego personelu. Z badań wynika też, że większość instytucji po prostu nie jest tego świadoma lub nie chce wiedzieć, czy też nie chce o tym rozmawiać[21]. W tym miejscu warto także zadać pytanie, czy zawsze komputer oraz internet jest wykorzystywany przez personel w trakcie godzin pracy do celów bezpośrednio związanych z wykonywanymi obowiązkami? Jest to ważna kwestia bezpieczeństwa nie tylko w kontekście państwa, ale społeczeństwa i gospodarki opartej na wiedzy.

W tym kontekście warto zauważyć, że aby przetrwać na konkurencyjnym rynku, większość firm korzysta z jakiejś formy analizy konkurencji, w celu zdefiniowania i zrozumienia mocnych i słabych stron konkurencji. Wiele informacji jest dostępnych publicznie i to stosunkowo prosta sprawa, aby je pozyskać i analizować[22].

Przemysł motoryzacyjny i lotniczy wraz z przemysłem stoczniowym, a przede wszystkim w sektorze inżynierii mechanicznej, są często celem ataków ze strony wywiadów gospodarczych. Część korporacji, która padła ofiarą wywiadu gospodarczego niechętnie przyznaje się do tego. Wynika to z pewnością z powodu, że takie zdarzenia mogą mieć negatywny wpływ na wartość akcji na giełdzie, a także na zaufanie klientów.

Często wywiad gospodarczy – przy pomocy byłych oficerów – korzysta z metod oraz doświadczeń wywiadu państwowego. Stosuje się często te same formy działalności, jak: podsłuch, kradzież i kopiowanie nośników pamięci, przechwytywanie e-maili, włamywanie się do sieci wewnętrznej, zdjęcia satelitarne, ale i także tradycyjne sposoby, jak: spotkania i kontakty na targach, konferencjach i sympozjach naukowych. Często także źródłem przecieków poufnych informacji są sami pracownicy instytucji lub kontrahenci.

Wywiad gospodarczy, obok wywiadu politycznego i militarnego, jest najczęstszą formą działania służb, bez względu na to czy reprezentują one reżimy

21 R. Bitton, *The legitimacy of spying among nations*, „American University International Law Review" 2014, nr 29/5, s. 1009–1070.

22 G. Brown, *Spying and Fighting in Cyberspace: What is Which?*, „Journal of National Security Law & Policy" 2016, nr 8/3, s. 1–22.

demokratyczne czy autorytarne. Jest on szeroko stosowany ze względu na swą opłacalność, zwłaszcza że zapewnia obniżenie kosztów badań i rozwoju poprzez odkrywanie tego, co już zostało osiągnięte przez innych, jednak nie wprowadzone jeszcze do użytku. A zatem pozyskanie nowej technologii jest o wiele tańsze i opłacalne niż jej skonstruowanie.

Polityka wewnętrzna

O znaczeniu wywiadu dla bezpieczeństwa państwa świadczy potrzeba prowadzenia polityki bezpieczeństwa, która jest jednym z kluczowych elementów sprawowania władzy. Czynnik ten we współczesnej historii Europy Środkowo-Wschodniej, a szczególnie w okresie transformacji ustrojowej, nabierał wyjątkowego znaczenia. Warto podkreślić, że Polska jest jednym z głównych celów rosyjskiego wywiadu, ze względu na fakt, że jest to państwo, którego granica wschodnia stanowi zewnętrzną granicę NATO i Unii Europejskiej. Polskie środowiska polityczne zaangażowały się w ostatnich latach w konflikt ukraiński oraz intensywnie promują dywersyfikację energetyczną Europy, co nie jest zgodne z interesami Moskwy. Skuteczny kontrwywiad jest niezbędny dla realizacji polityki państwa. Wyzwania, jakie stoją przed polskim kontrwywiadem wynikają przede wszystkim z trudnej i skomplikowanej historii, która kładzie się cieniem na relacje z sąsiadami, ponadto położenie geopolityczne sprawia, że Polska odgrywa często rolę państwa buforowego[23].

Służby wywiadowcze zainteresowane są szczególnie reorganizacją sił zbrojnych wynikającą z przynależności Polski do NATO, rozwojem infrastruktury przemysłu obronnego, zaawansowaną technologią, uzbrojeniem wojskowym, infrastrukturą transportową, a także efektami badań naukowych oraz zasobem surowców energetycznych. Wyzwaniem dla kontrwywiadu jest więc rywalizacja z obcą służbą, która posiada większe zasoby ludzkie i jest znacznie lepiej wyposażona.

W kontekście omówienia przydatności wywiadu dla organizacji państwowych, warto zastanowić się również, czy dla powstałych wojsk obrony terytorialnej przydatna może okazać się wiedza wywiadowcza. Organizacja ta ze swej natury jest formacją wewnętrzną, czyli działającą w granicach państwa.

23 M. Górka, *Rola i zadania kontrwywiadu w obszarze funkcjonowania państwa z uwzględnieniem wybranych aspektów polityki bezpieczeństwa III RP*, „Środkowoeuropejskie Studia Polityczne" 2017, nr 2, s. 103–123.

Trudno sobie wyobrazić, aby oprócz koniecznego sprzętu, oddziały tego typu nie posiadały wiedzy m.in. na temat współczesnych konfliktów, (w tym hybrydowych), ale i także o możliwościach, rozmieszczeniu i wyposażeniu wojsk państw sąsiednich. Naturalna jest więc potrzeba posiadania takiej wiedzy ze źródeł wywiadowczych[24].

Z definicji wywiad działa poza granicami państwa, a zatem można przypuszczać, że OT będzie korzystać z wiedzy służb wywiadowczych. Jednak dominującą rolę będzie odgrywać w tym przypadku kontrwywiad z racji tego, że zadania obu służb w określonym zakresie uzupełniają się. Przede wszystkim współpraca będzie dotyczyć eliminacji zagrożeń i przeciwdziałania służbom wywiadowczym obcych państw. Inną ważną rolą będzie zwalczanie działań organizacji separatystycznych czy też organizacji paramilitarnych, których celem jest destabilizacja państwa.

Bezpieczeństwo wewnętrzne państwa, choć należy w głównej mierze do obszaru zainteresowania służb kontrwywiadowczych, to jednak w kontekście pozyskiwania informacji ze strony tajnych służb, jest kluczowe dla stabilnego funkcjonowania państwa. Cała infrastruktura krytyczna, w tym sieci energetyczne, bankowość i systemy zaopatrzenia w wodę, komunikację i transport, są całkowicie uzależnione od sieci komputerowych. To powiązanie czy też uzależnienie od nowoczesnych technologii jest „pietą achillesową" każdego z rozwiniętych państw[25].

Przykładem tego może być paraliż informacyjny (wynikający z awarii informatycznej) jeśli chodzi o transport kolejowy, często więc dochodzi w takich sytuacjach do chaosu, agresji społecznej. Innym choćby przykładem są wyniki wyborów samorządowych w 2014 r., których oficjalne ogłoszenie przedłużyło się o kilka dni. Z tego też powodu dochodziło do licznych awantur, domysłów, a także opinii kwestionujących autentyczność wyników, a tym samym podważających zaufanie do państwa.

Zadaniem służb jest więc troska o bezpieczeństwo tego typu instytucji państwowych zarówno pod względem fizycznym, jak i cybernetycznym. Oznacza to, że infrastruktura krytyczna, ze względu na swoje zadania, jest podatnym celem ataków. W tym przypadku wymagana jest współpraca zarówno służb wywiadowczych, jak i kontrwywiadowczych. Z jednej strony wywiad

24 D.C. Stefanescu, *Military capabilities that Romania needs for preventing and waging a hybrid war*, „Review of the Air Force Academy" 2017, nr 1, s. 155–160.

25 R. Bossong, *The European Programme for the protection of critical infrastructures – metagoverning a new security problem?*, „European Security" 2014, vol. 23/2, s. 210–226.

gromadzi i przetwarza informacje o potencjalnych przeciwnikach w celu lepszego przygotowania się na ewentualny atak z ich strony oraz w celu złagodzenia możliwych szkód, które będą jego wynikiem. Z drugiej strony kontrwywiad podejmuje działania dotyczące ochrony przed szpiegostwem lub wewnętrznymi zagrożeniami, a także przed sabotażem będącym wynikiem działań wewnętrznej lub zewnętrznej siły, międzynarodowych działań terrorystycznych lub innych działań wywiadowczych o charakterze wojny informacyjnej bądź akcji dezinformacyjnych w cyberprzestrzeni[26]. Zagrożenia wymuszają stosowanie na większą skalę szkoleń, które miałyby uświadamiać pracowników instytucji publicznych o zagrożeniach związanych z bezpieczeństwem informacji i ich funkcjonowaniem w cyberprzestrzeni.

Terroryzm jako wyzwanie dla wywiadu

Praca wywiadu ewoluuje z upływem czasu. Pierwsza sprawa to nieprzerwany i dynamiczny postęp technologiczny, który daje narzędzia do pracy służbom, druga rzecz to – szczególnie w epoce zagrożeń terrorystycznych – zdobywanie danych nie tylko o przeciwniku, ale i o własnych obywatelach.

W walce z terroryzmem wywiad musi być pierwszy, a zatem musi wyprzedzać swoich wrogów. To także ogromna umiejętność przewidywania zdarzeń, która pozwala służbom na bycie kilka kroków przed przeciwnikiem, w przeciwnym razie służby mogą ponieść porażkę. Trzeba przewidzieć wiele możliwych scenariuszy i być przygotowanym na każdą ewentualność. To także praca dla osób, które starają się i potrafią zrozumieć logikę przeciwnika, wchodzą w jego rolę, dzięki temu dostrzegają słabości własnej strony.

Wywiad jest jako służba – w stosunku do pozostałych – pierwsza w walce z terroryzmem, pozostałe służby, jak oddziały specjalne, antyterroryści czy służby medyczne, mają charakter wtórny, w sensie etapu działania. To właśnie od pozyskania danych zależeć może udaremnienie zamachu[27]. Bardzo trudnym momentem jest także wybór odpowiedniego momentu aresztowania osoby podejrzanej o działalność terrorystyczną. Zbyt wczesna akcja może doprowa-

26 A. Barnea, *Counterintelligence: stepson of the intelligence discipline*, „Israel Affairs" 2017, vol. 23/4, s. 715–726.

27 A. D.M. Svendsen, *The Federal Bureau of Investigation and Change: Addressing US Domestic Counter-terrorism Intelligence*, „Intelligence and National Security" 2012, vol. 27/3, s. 371–397.

dzić do utraty możliwości wykrycia wszystkich członków organizacji terrorystycznej, natomiast zbyt późno podjęta akcja może skutkować zrealizowaniem zamachu, a tym samym tragedią[28].

Terroryzm jest współcześnie zjawiskiem, które najbardziej determinuje debatę publiczną. Problem zachowania bezpieczeństwa państwa jest szeroko omawiany w mediach, ale i również analizowany na poziomie wywiadu. I to właśnie analiza wywiadowcza daje szansę na udzielenie wiarygodnych odpowiedzi o źródła, jak i konsekwencje współczesnych zagrożeń. Paradoksalnie do opinii publicznej nie przedostają się informacje o udaremnionych zamachach, a takich przypadków jest znacznie więcej. Dlatego też trudno jest ocenić działalność służb bez posiadanej wiedzy. Głosy krytyczne pojawiają się dopiero przy towarzyszącej tragedii. Pewnym absurdalnym zjawiskiem jest fakt, że kiedy społeczeństwo jest zagrożone to opinia publiczna twierdzi, że służby słabo działają, ale jeśli społeczeństwo czuje się bezpieczne to zauważalna jest silniejsza krytyka wobec służb m.in. za stosowanie narzędzi wywiadowczych jak np. podsłuchy.

Wymownym przykładem, który mówi wiele o roli wywiadu jest polityka antyterrorystyczna. Przed zamachem z 13 listopada 2015 r. w Paryżu istniały bardzo duże problemy w wymianie informacji między Francją a Belgią. Warto podkreślić, że zamach ten planowano w Brukseli. Belgia w tym czasie miała bardzo nieskuteczne służby bezpieczeństwa – co zresztą bardzo skrzętnie wykorzystali terroryści. Ponadto w Brukseli poszczególne oddziały policji nie wiedziały co robią pozostałe. W takiej sytuacji trudno jest wyłapywać sygnały o zagrożeniu[29]. Istnieje zatem potrzeba zbudowania systemu zbierania i przepływu danych. Jeśli nawet służby greckie lub bułgarskie zidentyfikują kogoś kto wjeżdża do UE z terytorium Turcji, ale przedtem był w Syrii lub w Iraku, to nie jest jeszcze sukces. Sukcesem dopiero będzie, jeśli ta informacja dotrze do służb pozostałych krajów UE. Bez takiej wiedzy służby pozostałych państw nie będą wiedziały w ogóle o istnieniu takiej osoby, nie mówiąc już o miejscu jej pobytu oraz zamiarach. Kluczowa w polityce antyterrorystycznej jest więc wymiana informacji[30].

28 S. Sloan, *Meeting the Terrorist Threat: The Localization of Counter Terrorism Intelligence*, „Police Practice and Research" 2002, vol. 3/4, s. 337–345.

29 S. Lefebvre, *„The Belgians Just Aren't up to It": Belgian Intelligence and Contemporary Terrorism*, „International Journal of Intelligence and CounterIntelligence" 2017, vol. 30/1, s. 1–29.

30 M. Górka, *Wybrane aspekty polityki bezpieczeństwa w kontekście zagrożeń terrorystycznych w Europie*, „Symbolae Europaeae" 2017, nr 11, s. 64.

Znaczenie wywiadu dla misji pokojowych

Współcześnie granica między pokojem a wojną stała się niewyraźna. Potrzeba wywiadu podczas operacji pokojowych jest oczywista zarówno w celu zapewnienia bezpieczeństwa wojsk, jak i zwiększenia szans na powodzenie misji. Jedną z głównych zalet operacji pokojowych jest bezpośredni dostęp do obszaru i jego mieszkańców oraz interakcji ze zwaśnionymi stronami. Ważne informacje mogą być nabywane poprzez rozmowę z tubylcami i ich obserwację. Informacje te są trudne do uzyskania przez tradycyjne środki wywiadowcze. Jak pokazuje przykład misji w Somali, kobiety i dzieci na ogół dostarczały więcej informacji niż robili to płatni i profesjonalni informatorzy. Jak zawsze w przypadku korzystania z osobowych źródeł informacji (HUMINT), ochrona tożsamości źródła jest niezbędna. Ponadto w przypadku konfliktu, gdzie niektóre strony nie wahają się zabijać cywilów, jak to miało miejsce w latach 90. XX wieku w byłej Jugosławii czy w Rwandzie, konieczne jest unikanie zdarzeń dających powody lokalnym reżimom do zabijania ludności cywilnej.

Siły pokojowe muszą przekonać skonfliktowane strony, że głównym ich celem jest ułatwienie negocjacji pokojowych. Często muszą one brać pod uwagę niezwykle delikatną sytuację, w której np. pojedynczy strzał może wywołać szereg kontrowersji na szczeblu dyplomatycznym. W niektórych przypadkach głównym zadaniem jest niesienie pomocy w nieprzyjaznym środowisku jak np. w Bangladeszu czy w Somalii. W innych przypadkach celem misji jest oddzielenie dwóch walczących armii jak to miało miejsce na półwyspie Synaj. Czasami linia konfrontacji jest niewyraźna, wyznaczana bywa według walczących grup etnicznych na dużej powierzchni jak to było w przypadku Bośni[31].

Wywiad w operacji pokojowej różni się w istotny sposób od wywiadu podczas działań wojennych. Metody zbierania danych są niesłychanie bardziej wrażliwą sferą niż podczas konfliktu. Wykrycie prowadzonych działań wywiadowczych może podważyć zaufanie do sił pokojowych, a tym samym może to w negatywny sposób wpływać na współpracę. Zawsze też pojawią się osoby, które będą oskarżać siły pokojowe o szpiegostwo i stronniczość. Zdarzają się jednak sytuacje, w których skonfliktowane strony uważają, że mają powody, aby sądzić, że poprzez organizacje pokojowe przedostają się informacje do przeciwników. Przyczyny takiego stanu wynikają z tego powodu, że misje ONZ

31 J.A. Edwards, J.M. Valenzano, K. Stevenson, *The Peacekeeping Mission: Bringing Stability to a Chaotic Scene*, „Communication Quarterly" 2011, vol. 59/3, s. 339–358.

składają się głównie z krajowych kontyngentów, które są w rzeczywistości kontrolowane przez rządy tych państw[32].

Warto zauważyć, że potrzeby wywiadowcze określone przez ONZ nie zawsze są akceptowane przez poszczególne państwa. Czasami warunkowo dowódcy mogą zdecydować, że dotychczasowe rozpoznanie na podstawie informacji z ONZ jest niewystarczające dla zapewnienia bezpieczeństwa swojej jednostce i dlatego zmuszeni są do zainicjowania niezależnych operacji wywiadowczych. Siły pokojowe mogą mieć także interesy i powiązania, które są sprzeczne z wyraźnymi celami mandatu, a czasem nawet wbrew oficjalnej retoryce danego państwa. Przykładem tego jest konflikt w byłej Jugosławii. ONZ wykazało, że podczas operacji niektóre rządy nie wahały się dołączyć do operacji jednostek wywiadu, będących poza kontrolą ONZ. Informacje wywiadowcze zbierane pod pretekstem misji pokojowych mogą być więc przeznaczane w celu zaspokajania potrzeb określonego państwa[33].

Niemniej jednak informacje, które są prawidłowo używane i wykorzystane, mogą zapewnić znacznie lepszy obraz funkcjonowania sił pokojowych, szczególnie na poziomie operacyjnym i taktycznym. Wywiad jest niestety bardzo fragmentaryczny, ponieważ jednostki pokojowe często nie mają ani pełnej kontroli nad ich obszarem działalności, ani też wielkiego wyboru co do metod zbierania danych.

Typowa wiedza wywiadowcza podczas misji pokojowych sprowadza się do pozyskiwania danych na temat sytuacji etnicznej, społeczno-ekonomicznej oraz postawy liderów lokalnych. Pomaga to uniknąć błędów kulturowych, jak choćby przy okazji powitań i prowadzenia rozmów żołnierzy z kobietami, czy też częstowania jedzeniem muzułmańskich przywódców w czasie Ramadanu[34].

Wywiad musi także posiadać informację, która pozwoli odpowiedzieć na pytania: dlaczego pewne obszary objęte konfliktem reagują niekorzystnie niż inne na obecność sił pokojowych? Jakie są historyczne oraz obecne powiązania pomiędzy daną społecznością a innymi grupami społecznymi? Czy na wskazanym terytorium obecne są nacjonalistyczne bądź fundamentalistyczne organizacje? Z której ze stron można spodziewać się czystek etnicznych? Czy

32 R.D. Steele, *Peacekeeping Intelligence and Information Peacekeeping*, „International Journal of Intelligence and CounterIntelligence" 2006, vol. 19/3, s. 519–537.

33 P. Shetler-Jones, *Intelligence in Integrated UN Peacekeeping Missions: The Joint Mission Analysis Centre* „International Peacekeeping" 2008, vol. 15/4, s. 517–527.

34 T. Woodhouse, *Peacekeeping, Peace Culture and Conflict Resolution*, „International Peacekeeping" 2010, vol. 17/4, s. 486–498.

siły międzynarodowe postrzegane są jako przyjaciel czy wróg? Są to oczywiście wybrane pytania, których jest o wiele więcej, jednak pokazują one rozmiar i zasięg problemów, z którymi musi zmierzyć się wywiad i który wyposaża w wiedzę siły pokojowe.

Zakończenie

Pojawienie się cybertechnologii wywarło głęboki wpływ na cykl wywiadowczy w zakresie sposobu działania wywiadu oraz na jego interakcje z decydentami politycznymi. Rewolucja informacyjna wpłynęła również na sposób, w jaki decydenci polityczni mają dostęp do wiarygodnych informacji i źródeł, w oparciu o które podejmowane są decyzje. Ewolucja systemów wywiadowczych umożliwiła natychmiastowy wgląd do dotychczas trudno dostępnych miejsc, w których znajdują się nieprzetworzone informacje.

Wywiad polega na systematycznym i ciągłym procesie gromadzenia, przetwarzania, analizowania i rozpowszechniania potrzebnych informacji wywiadowczych o znaczeniu strategicznym, w celu ułatwienia opracowania i wdrożenia strategii i planów na poziomie państwowym, regionalnym i międzynarodowym. Jest zatem użytecznym narzędziem w tworzeniu strategii bezpieczeństwa narodowego w celu zapobiegania lub ograniczania zróżnicowanych zagrożeń dla państwa i jego obywateli lub w celu wykorzystania możliwości wynikających ze stosunków geopolitycznych, regionalnych i międzynarodowych ram bezpieczeństwa.

Wywiad stanowi ważne narzędzie w działaniach informacyjnych i wspierających decydentów politycznych. Aby sprostać zwiększonemu oczekiwaniu władz oraz presji szybkiego gromadzenia nieprzetworzonych danych, wywiad musi stale opracowywać nowe rozwiązania w zakresie zdolności gromadzenia danych, zarządzania informacjami, wykorzystywania alternatywnych metod analizy, zwiększania i udoskonalania analiz długoterminowych, czy też dostosowywania procesów i środków przekazu swoich produktów do potrzeb i oczekiwań decydentów politycznych.

Pierwsze miejsce w wywiadzie zawsze będzie odgrywać informacja. To ona decyduje o przewadze czy też o zwycięstwie w rywalizacji między podmiotami. Wiedza pozwala władzom lepiej funkcjonować i mieć znacznie większe poczucie bezpieczeństwa. Nowe postrzeganie i rozumienie świata polega na przekraczaniu lub też odrzuceniu sztywnych granicy państwowych i dostosowywaniu się do nowych trendów światowych. Agencje bezpieczeństwa, które

do tej pory działały na polu międzynarodowym, szukają zewnętrznego wroga wewnątrz granic własnego państwa, natomiast instytucje działające w sferze bezpieczeństwa wewnętrznego coraz częściej realizują swoje zadania poza granicami państwa.

Wykorzystanie treści pochodzących z otwartych źródeł informacji oraz opracowanie protokołów zbierania danych dotyczących internetowych portali społecznościowych stanowi jedno z głównych wyzwań wywiadu. Ich realizacja stała się obecnie jednym z kluczowych czynników zapewniających dostarczanie informacji decydentom politycznym. Gwarantuje również skuteczne prowadzenie działań przeciwko podmiotom zagrażającym interesom narodowym.

Bibliografia

Barnea A., *Counterintelligence: stepson of the intelligence discipline*, „Israel Affairs" 2017, vol. 23/4.

Berliński M., Zulczyk R., *Federalna Służba Bezpieczeństwa Federacji Rosyjskiej*, Warszawa 2016.

Bielska A., Smółka P. (red.), *Wywiad biznesowy*, Piaseczno 2017.

Bitton R., *The legitimacy of spying among nations*, „American University International Law Review" 2014, nr 29/5.

Bossong R., *The European Programme for the protection of critical infrastructures – meta-governing a new security problem?*, „European Security" 2014, vol. 23/2.

Brown G., *Spying and Fighting in Cyberspace: What is Which?*, „Journal of National Security Law & Policy" 2016, nr 8/3.

Degaut M., *Spies and Policymakers: Intelligence in the Information Age*, „Intelligence and National Security" 2016, vol. 31/4.

Edwards J.A., Valenzano J.M., Stevenson K., *The Peacekeeping Mission: Bringing Stability to a Chaotic Scene*, „Communication Quarterly" 2011, vol. 59/3.

Fripp W., *The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age*, „Intelligence and National Security" 2018, vol. 33/4.

Górka M. (red.), *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa: historia i współczesność*, Toruń 2016.

Górka M. (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa 2016.

Górka M., *Dyplomacja i wywiad. Przyczynek do refleksji nad polityką bezpieczeństwa* [w:] M. Górka (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa 2016.

Górka M., *Mossad. Porażki i sukcesy tajnych służb izraelskich*, Warszawa 2015.

Górka M., *Rola i zadania kontrwywiadu w obszarze funkcjonowania państwa z uwzględnieniem wybranych aspektów polityki bezpieczeństwa III RP*, „Środkowoeuropejskie Studia Polityczne" 2017, nr 2.

Górka M., *Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa*, „Systemy wspomagania inżynierii produkcji" 2017, vol. 6/5.

Górka M., *Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 roku*, „e-Politikon" 2017, nr 19.

Górka M., *Wybrane aspekty polityki bezpieczeństwa w kontekście zagrożeń terrorystycznych w Europie*, „Symbolae Europaeae" 2017, nr 11.

Gruszczak A., *Europejska wspólnota wywiadowcza. Prawo – instytucje – mechanizmy*, Kraków 2014.

Kahana E., *Mossad – CIA Cooperation*, „International Journal of Intelligence and CounterIntelligence" 2010, vol. 23/2.

Lahneman W.J., *The Need for a New Intelligence Paradigm*, „International Journal of Intelligence and Counterintelligence" 2010, vol. 23/2.
Larecki J., *Wielki leksykon tajnych służb specjalnych świata*, Warszawa 2017.
Lefebvre S.,*„The Belgians Just Aren't up to It": Belgian Intelligence and Contemporary Terrorism*, „International Journal of Intelligence and CounterIntelligence" 2017, vol. 30/1.
Mattern T., Felker J., Borum R., Bamford G., *Operational Levels of Cyber Intelligence*, „International Journal of Intelligence and CounterIntelligence" 2014, vol. 27/4.
Minkina M., *FSB. Gwardia Kremla*, Warszawa 2016.
Minkina M., Gałek B., *Gry wywiadów. Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015.
Minkina M., *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Warszawa 2014.
Minkina M., *Wywiad Federacji Rosyjskiej*, Siedlce 2012.
Omilianowicz R., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej* [w:] W. Wróblewski, *Wywiad i kontrwywiad w świecie*, Szczecin 2009.
Pawlikowicz L., *Aparat centralny 1 Zarządu Głównego KGB jako instrument realizacji globalnej strategii Kremla 1954–1991*, Warszawa 2013.
Rudner M., *Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge*, „International Journal of Intelligence and CounterIntelligence" 2013, vol. 26/3.
Shetler-Jones P., *Intelligence in Integrated UN Peacekeeping Missions: The Joint Mission Analysis Centre* „International Peacekeeping" 2008, vol. 15/4.
Shimron G., *The Mossad and the Myth*, Tel Awiw 1996.
Siemiątkowski Z., *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009.
Sloan S., *Meeting the Terrorist Threat: The Localization of Counter Terrorism Intelligence*, „Police Practice and Research" 2002, vol. 3/4.
Steele R.D., *Peacekeeping Intelligence and Information Peacekeeping*, „International Journal of Intelligence and CounterIntelligence" 2006, vol. 19/3.
Stefanescu D.C., *Military capabilities that Romania needs for preventing and waging a hybrid war*, „Review of the Air Force Academy" 2017, nr 1.
Stephens E., *Caught on the hop: the Yom Kippur war*, „History Today" 2008, vol. 58/10.
Svendsen D.M., *The Federal Bureau of Investigation and Change: Addressing US Domestic Counter-terrorism Intelligence*, „Intelligence and National Security" 2012, vol. 27/3.
Tyler P., *Twierdza Izrael. Zakulisowa historia elit wojskowych, które uparcie bronią się przed pokojem*, Poznań 2014.
Wilner A., *Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation*, „Comparative Strategy" 2017, vol. 36/4.
Woodhouse T., *Peacekeeping, Peace Culture and Conflict Resolution*, „International Peacekeeping" 2010, vol. 17/4.
Wróblewski W. (red.), *Wywiad i kontrwywiad w świecie*, Szczecin 2009.

Informational actions of the intelligence within the scope of the safety policy, including cyberspace

Abstract

The enormous changes and constant developments in the applications of technology and communication have changed the way the world is perceived. The information revolution has impacted on intelligence gathering, processing, analysis and dissemination, as well as on how decision-makers can access reliable information in a timely manner, and on the sources they are likely to rely on when concrete information is needed to make decisions. This article attempts to describe, analyse and explain the nature of the ongoing information revolution, its main impact on intelligence and security policy, and the importance of intelligence analysis in the context of peacekeeping operations.

Key words: security policy, intelligence, counter-intelligence, cyber-security, peacekeeping missions, informationprocessing, communication, technological development, foreign policy

Katarzyna Chałubińska-Jentkiewicz*

Responsibility on the network – the diagnosis of the current state

Abstract

The article deals with the diagnosis of the current state in relation to responsibility in the flexible area of cyberspace which is itself hard to define, in the context of security, especially its transsectoral informative part; Polish statutory, strategic and program solutions are presented in the light of EU standards. The study includes a review of threats (mainly information and ICT infrastructure) and their scopes (systemic, economic, socio-cultural) and addressees obliged to preventive and eradication activities (primarily public authorities, but also other, e.g. commercial entities or representatives operating on the market of information society); it also touches on the substantive and institutional cooperation issues at the European level.

Key words: cyberspace, cybersecurity, responsibility, threats, informationsociety, informationinfrastructure, ICT infrastructure, communication, newtechnologies

* Dr hab. prof. nadzw. Katarzyna Chałubińska-Jentkiewicz, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, kierownik Katedry Prawa Mediów, Własności Intelektualnej i Nowych Technologii, e-mail: kasiachalubinska@gmail.com.

The dynamic civilizational changes which have been observed in recent years all over the world are the result of the rapid and dynamic development of information technologies as well as communication technologies which support them. Thus, cyberspace is a new sphere of the influence of these processes as the fifth area of defense activities. According to W. Kitler, the fields of security may have their own separateness and be related to specific sectors of the state, but there are-and there will be more and more of them-which are not industry-specific, but trans-sectoral, trans-disciplinary. These include, for example: information, cybernetics, anti-terrorism, political system, classified information security[1].

Generally speaking, security can be perceived primarily in a negative sense as a state characterized by the absence of threats, but also the absence of dangers, certainty, peace, protection against threats[2].

Security can be achieved by protecting the state's information resources against hostile activities of the enemy (disinformation and propaganda), as well as maintaining the ability for offensive, immediate actions against the perpetrators of these activities. The term 'network and information security' is defined in Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency as' the resistance of a network or information system to accidental events or illegal or deceptive activities affecting the availability, authenticity, integrity and confidentiality of data stored or transmitted, and related services offered or available through these networks and systems[3].

It should be emphasized that information security as only one of the elements of cybersecurity has been subject to regulations under criminal law (see – Offences against information – chapter 33 of the Penal Code[4]), provisions of the Personal Data Protection Act and the Act on the Protection of Classified Information. All social interactions have an impact on security, and the so-called "security culture" itself determines what the attitude to risk, threats and security of a given community is, and what values in this regard are

1 Zob. Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej, BBN, Warszawa 2013, s. 19 (rys. 1).

2 Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne.

3 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję do spraw Bezpieczeństwa Sieci i Informacji.

4 Kodeks karny z dnia 6 czerwca 1997 r. (t.j. Dz.U. z 2018 r., poz. 1600 ze zm.).

considered to be significant. The basic design of the internet is based on the openness of both its infrastructure architecture and the culture of its creators and users. The simplicity and easiness of connecting various computers has allowed a huge increase in the number of users, and the open philosophy of its creation has built a huge, multi-level interactive medium[5].

Cybercrime is a relatively recent phenomenon, but it is developing rapidly. Currently, almost everyone has access to use the ICT network and its resources. Therefore, cybercrime, due to the increasingly common access to the network, may harm the interests of the state, which transfers some of its affairs to the field of the ICT network, which sometimes can even lead to undermining state's sovereignty[6].

It happens because not all users of data communication networks understand the mechanisms of the ICT network well, which leads to a kind of ignorance of their own security in cyberspace. We should remember that cyber crime includes both acts that reflect crime in the real world and completely new phenomena that are unique to cyberspace[7] and pose threats to the individual or the state. The main report on threats to national security identifies about 50 types of threats, with 18 of them included in the National Crisis Management Plan, the threat of cyber terrorism among them[8]. In the case of cyber attacks, only the possible effects of cyber attacks on people and property are mentioned and they include potential consequences for the population which are: threat to human life and health caused by disruptions of energy systems, traffic control, etc., loss of trust in public institutions, inability to perform professional tasks, inability to communicate.

As the potential consequences of cyber attacks in regard to properties one mentions the following: significant financial and economic losses as well as social effects, disruptions in the supply of energy, fuels, food, drinking water, and disruption to the operation of the transmission infrastructure.

In turn, crisis management covers ICT networks, but more as one of the types of transmission networks, and at the same time does not take into account the layer of sharing, processing and storing information that permeates all aspects

5 T. Goban-Klas, *Cywilizacja medialna*, Warszawa 2005, s. 151.

6 M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno-karne*, Warszawa 2011, s. 24.

7 K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii*, Warszawa 2015, s. 353.

8 Online <http://rcb.gov.pl/raport-o-zagrozeniach-bezpieczenstwa-narodowego-3/>.

of the functioning of the information society. The following main categories and subcategories of threats were adopted in the report on Cyberspace Risk Assessment in Government Administration in 2013: information-oriented threats (information theft for publication or sale, information counterfeiting), threats focused on IT infrastructure (data deletion, disruption of functioning, taking over the IT systems), IT failures, insufficient competence[9].

The regulators' approach to the issue of cyberspace, cyber security and cyber responsibility results from identifying this type of protection with the need to counteract attacks directed at networks themselves, which seems unjustified, especially in the context of analyzing the concept of cyberspace[10].

The above-mentioned understanding of the notion of cyberspace entered the legal language together with the introduction of the Act of August 30, 2011 amending the Act on Martial Law and on the competences of the Supreme Commander of the Armed Forces and the rules of its subordination to the constitutional organs of the Republic of Poland and some other acts[11]. The Polish definition of the concept of cyberspace is found in the Act of 29 August 2002 on Martial Law and the powers of the Supreme Commander of the Armed Forces and the principles of its subordination to the constitutional organs of the Republic of Poland[12]. Another legal definition of the concept of cyberspace is contained in the Act of 21 June 2002 on the state of emergency[13]. According to the above Act, cyberspace is understood as "the space of processing and exchange of information created by ICT systems specified in art. 3 point 3 of the Act of 17 February 2005 on the computerization of the activities of entities performing public tasks[14], together with the connections between them and relations with users"[15].

9 System bezpieczeństwa cyberprzestrzeni RP, NASK/CERT Polska, s. 62, Warszawa, wrzesień 2015 r. <https://mac.gov.pl/files/nask_rekomendacja.pdf>.

10 Zob. więcej na ten temat: K. Chałubińska-Jentkiewicz, *Cyberprzestępczość jako paradygmat pojęcia bezpieczeństwa w cyberprzestrzeni*, „Wojskowy Przegląd Prawniczy" 2016, nr 3, s. 46–64.

11 Dz.U. nr 222, poz. 1323.

12 Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. nr 156, poz. 1301).

13 Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985)

14 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).

15 Art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym.

The same legal definition is contained in the Act of 18 April 2002 on the state of natural disaster[16]. These laws apply to virtual reality in which legal entities move when martial, emergency or natural disaster states take place. The concept of the national cyber security system adopted in the Assumptions of the Cybersecurity Strategy of the Republic of Poland includes, inter alia, rebuilding the definition of cyberspace and its extension to the sphere of key operators functioning in the economic sphere.

The concept of cyberspace can therefore be defined as a synthesis of all physical and technical means which enable the exchange information electronically as well as the relationships of its users having access to its resources.

Cybersecurity or network security is a term referring to providing protection and counteracting threats that affect cyberspace itself as well as functioning of subjects in cyberspace in both public and private sectors as well as their mutual relations. However, according to Act 2 point 4 of the Act of 5 July 2018 on the national cyber security system[17] – cybersecurity means the resistance of information systems to activities violating the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems. Therefore, this definition comprises the issues of technical nature and network protection as such. On the other hand, in favour of this position, one can also find the definition of cybersecurity in much broader, interdisciplinary perspective including all incidents which occur in cyberspace [18]. The incident pursuant to art. 2 point 5 of the Act on the national cybersecurity system is an incident – an event which has or may have an adverse effect on cybersecurity. However, according to art. 2 point 6 a critical incident is an incident resulting in significant damage to safety or public order, international affairs, economic benefits, public institutions activities, law and civic rights and freedoms as well as to people's life and health properly classified by the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV.

16 Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558).

17 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

18 Zaznaczyć także trzeba, że jednym z wciąż podstawowych problemów dotyczących odpowiedzialności w sieci jest zagadnienie jurysdykcji terytorialnej, która znalazła zastosowanie w przepisach Konwencji o cyberprzestępczości. Problemy z ustaleniem osoby przestępcy, a jak wiadomo większość przestępstw popełnianych jest w innych państwach niż faktyczne miejsce przebywania przestępcy, utrudnia działania związane z efektywnością ścigania cyberprzestępczości.

To go into further distinction of incidents, we can talk about a major incident which is an incident that causes or may cause a serious reduction in quality or interruption of the key service provision; crucial incident – an incident that has a significant impact on the provision of a digital service within the meaning of Art. 4 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council with regard to further clarifying the elements to be taken into account by digital service providers in managing existing risks for the security of network and information systems, and parameters to determine whether an incident has a significant impact, hereinafter referred to as "Implementing Regulation 2018/151"[19].

An incident in a public entity -an incident that causes or may cause a reduction in quality or interruption of the implementation of a public task being carried out – these are activities that enable detection, recording, analyzing, classifying, prioritizing, taking corrective actions and reducing the effects of an incident.

The whole complexity of these issues parallels the issues happening in the real world. Thus, the legislators at various levels, both international and national, are introducing new regulations. In consequence, any kind of the phenomenon of impunity for illegal activities is no longer possible on the net. It should be noted that cyberspace in terms of adopting or creating new rules of behaviour is more flexible than reality. This unique ability of cyberspace brings comfort and completely new challenges to the legislator. The convenience is the ease of introducing regulations adequate to those in force in the real world, but the provisions so established often face blocking or ordinary ignorance on the part of ICT network users, in particular due to the lack of instruments for pursuing claims or prosecuting crime. One of the key problems is to identify entities responsible for ensuring cybersecurity, entities responsible for illegal activities on the network, mainly related to the provision of services, and for undesirable effects that are the result of computer activity. These three areas determine three directions of research related to responsibility in cyberspace.

Cyberspace is nowadays a symbol of development, but also freedom and privacy, and every interference in its functioning is associated with an attack on these values. In the countries involved in building the information society, cyberspace security is recognized as one of the most serious challenges in

19 Odpowiedzialność w cyberprzestrzeni RP (Dz.Urz. UE L 26, s. 48).

the national security system. It refers to both the security of the entire state institution and individual citizens. That is why public tasks for cyberspace security occupy an important place in the National Security System of the Republic of Poland. The responsibility for ensuring cybersecurity rests with all network users, but with no doubt, public administration bodies play a crucial role in providing actions to ensure public security and order.

As previously mentioned, one of the priority public tasks is to ensure the security of cyberspace as a cross-sectoral area. Cybersecurity is important because threats in cyberspace can negatively affect national needs, and their implementation is the essence of public tasks. The most important national needs include: systematic needs (e.g. strengthening of the socio-economic system and legal order), economic needs (e.g. development of the country, economic growth), social needs (ensuring health protection, social security, and counteracting all forms of discrimination), ecological needs (environmental protection) and cultural needs (nurturing national heritage, respecting ideological and ethnic differences) [20]. All possible cyber threats can affect each of these national needs negatively and it explains why cyberspace security is so important for the proper functioning of the state. Public tasks in the field of cyberspace security are implemented primarily through the cooperation of public authorities and services responsible for cybersecurity both at the national (private sector, non-governmental organizations) and international (NATO, European Union, UN, transnational associations)[21]. Another important element of these tasks are legislative activities, i.e. the preparation of appropriate legal provisions protecting cyberspace and thus reducing the risk of potential attacks[22]. The strategic tasks in the field of cyberspace security include: combating threats in cyberspace; protection of state information systems; cooperation with the private sector (mainly telecommunications) in the scope of providing information on cyber threats; proactive and preventative actions in the field of citizens' security against cyber threats; tracking cyber crimes and prosecuting their perpetrators; conducting both offensive and defensive information activities in cyberspace,

20 W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011, s. 37.

21 P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 244.

22 A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyber-terroryzmem*, Warszawa 2012, s. 21.

as well as cooperation with other entities of the National Security System of the Republic of Poland[23].

Thus, various types of state entities, guards, services and inspections reporting to the Prime Minister or individual ministers are obliged to fulfil public tasks in order to maintain cyber safety. The leading role among them, due to their competences, is played by the Internal Security Agency, the Minister of Digitization, the Minister of the Interior and Administration and the Minister of National Defense. There are also many other public authorities responsible for this zone, such as the President of the Office of Competition and Consumer Protection.

However, the Minister of National Defense plays a key role in the security of cyberspace. With the development of digitization of public administration, the Armed Forces have also undergone the process of computerization and as a result, it led to the emergence of sensitive points vulnerable to attacks from cyberspace[24]. New technologies and networks are used more and more often in operational reconnaissance[25] or information struggle. These processes are intensifying with the development of nanotechnology and automated and robotic devices. It should be noted that offensive operations also penetrate cyberspace, which means that more countries are deciding to develop digital offensive capabilities designed to deter potential aggressors[26]. Changes related to digitization resulted in the creation of special units dealing with cyberspace security in the structures of the Polish Armed Forces. As part of the General Staff of the Polish Army, under the leadership of the General Commander of the Armed Forces, there is the Information Systems Inspectorate connecting individual IT support units that operated until October 1, 2013. The creation of the Information Systems Inspectorate clarified the responsibility for the IT security management system in cyberspace, which is the responsibility of the Minister of National Defence. The General Staff of the Republic of Poland performs other tasks in the field of cyberspace security with the help of the Command and Communications Systems Planning Board. The newly created unit reporting to the Ministry of National Defence is the National

23 Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa, 2013, s. 250, <http://www.spbn.gov.pl/>, s. 63.

24 P. Bączek, *Zagrożenia*..., s. 136.

25 M. Sadlok, *Cyberterroryzm, cyberprzestępczość – wirtualne czy realne zagrożenie?*, <http://www.racjonalista.pl/kk.php/s,846>.

26 M. Grzelak, K. Lidel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 128.

Cryptology Center, which deals with research and implementation of cryptographic solutions for the needs of the Polish public administration and the army. The Cybernetic Operations Center is being created as part of the National Cryptology Centre. Another important body that performs tasks to ensure the security of cyberspace is the President of the Office of Electronic Communications, which is a regulatory body in the field of telecommunications and postal services, and NASK which is responsible for cyber security. As a consequence of the development of these services, the Minister of Internal Affairs plays an extremely important role for cybersecurity and public order in cyberspace and the Chief Commander of Police plays a key role under the supervision of the former. There is a special department within the Headquarters of Police called the Support Unit for Fighting Cybercrime and it deals with internet crime detection, analysis of cyberspace incidents, exchange of information and cooperation with national and international subjects.

Moreover, it should be pointed that telecommunication entrepreneurs and network operators need new regulations in their work as well. It is hard to deny that the ability to monitor transactions and activities carried out by network users and to get information about financial operations, commercial behavior and decisions, consumer habits, etc. poses a serious threat to privacy, personal data protection, and generally a sense of security of the individual. The global extent of the telecommunication services contributes to the lack of full legal regulations in this area. Due to the fact that this type of services is cross-border hence local, national legal systems are not always valid in other countries. Furthermore, the market of telecommunication services is very different from traditional service market and that is why it requires totally different, innovative attitude towards legal regulations. Digital service market does not have the subsidiary character any longer in comparison to traditional service market because the internet became a crucial element of economic life and an important tool in the process of globalization of the services. Thus, new legal problems in electronic commerce "appeared as soon as the initial naïve belief (or hope) developed that most of the internet would be a kind of freedom without rigid legal frameworks, administrative restrictions or fiscal burdens"[27].

27 J. Barta, R. Markiewicz, *Wstęp* [w:] J. Barta, R. Markiewicz (red.), *Handel elektroniczny. Problemy prawne*, Kraków 2005, s. 10.

Thus, it can be said that in recent years we have observed an increase in public administration's interest in cyberspace security, which means that more and more units and organizations dealing with this problem are being created. However, for more effective performance of public tasks in this area, cooperation and exchange of information between administrative, military and civilian areas is necessary. The European Union Cybersecurity Strategy: open, secure and protected cyberspace[28] proposes the creation of a network of national cybersecurity authorities. According to the EU strategy, national network and information security authorities should cooperate and exchange information with other regulatory authorities, in particular with personal data protection authorities, and regularly publish non-classified information on current early incidents and threats on a dedicated website and coordinated responses. According to the European Commission, legal obligations should not replace or prevent informal and voluntary cooperation, including cooperation between the public and private sectors, aimed at increasing the level of security and the exchange of information and best practices. A particularly important and useful platform at EU level to be developed is the European Public-Private Partnership on Resilience[29].

The above-mentioned tasks of public entities, however, do not make the list of necessary conditions related to the protection of national security in the digital age. However, responsibility for online activities has a cross-sectoral dimension. In the EU strategy "Cybersecurity strategy of the European Union: open, secure and protected cyberspace", which the European Commission published on February 7, 2013 as a joint communication of the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "The European Union Cybersecurity Strategy: Open, secure and protected cyberspace", it was found that private entities still lack effective incentives to provide reliable data on incidents in terms of network and information security and their effects, to the system speech prevention and to invest in security solutions. The purpose of the proposed legal act is therefore to bring about a situation in which entities operating in

28 COM (2013) z 7 lutego 2013 r. JOIN(2013) 1 final.

29 Europejskie partnerstwo publiczno-prywatne na rzecz odporności zostało zainicjowane na podstawie dokumentu COM(2009) 149. Platforma ta zainicjowała działania i intensywniejszą współpracę między sektorem publicznym i sektorem prywatnym w zakresie identyfikacji kluczowych zasobów, środków, funkcji i podstawowych wymogów w odniesieniu do odporności, jak również zapotrzebowania na współpracę i mechanizmy reagowania na zakrojone na szeroką skalę zakłócenia łączności elektronicznej.

many key areas (energy, transport, banking, stock exchanges, technologies enabling the provision of key internet services, as well as public administration bodies) assess cybersecurity threats, based on which are exposed, ensure the reliability and resilience of networks and information systems using appropriate threat prevention strategies, and exchange information with relevant network and information security authorities. Systemic prevention of threats in the field of cybersecurity can contribute to increasing economic opportunities and competitiveness in the private sector, making cybersecurity one of the advantages of the services offered. These entities will be required to report incidents to the competent national authorities on network security and information that have a significant impact on the continuity of basic services and the supply of goods dependent on networks and information systems.

The strategy highlights the need to promote dialogue and coordination between civil and military subjects in the EU, placing particular emphasis on the exchange of good practices, exchange of information, early warnings, response to incidents, threat assessment, information activities, and making cybersecurity a priority; ensuring dialogue with international partners, including NATO, and with other international organizations and multinational centers of excellence to ensure effective defense capabilities, identify areas of cooperation and avoid duplication of efforts.

According to the European Commission, the responsibility for increasing security in cyberspace rests with all entities that create the global information society, from citizens to government administrations. The EU supports actions aimed at defining norms of behavior in cyberspace to which all interested parties should comply. Just as the EU expects citizens to comply with civil and social norms and online law, states should also comply with applicable norms and regulations. In matters of international security, the EU encourages support for actions to build confidence in cybersecurity to increase transparency and reduce the risk of false perceptions of your actions. The legal obligations contained in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should also be respected online. The EU will focus on how to ensure that these obligations are also enforced in cyberspace. As regards the fight against cyber crime, the Budapest Convention, which is open for adoption by third countries, is an appropriate instrument. It is a model for national legislation in the field of cybercrime and is the basis for international cooperation in this

field. If armed conflicts extend to cyberspace, international humanitarian law and human rights law will apply.

Directive 2016/1148 is the first EU law in the field of cybersecurity introducing cross-sectoral regulations. The time to implement the directive in the legal systems of the member states expired on May 9, 2018. The text of the directive focuses on three pillars: 1) institutions that should be established in all Member States; 2) cooperation at European level; 3) obligations regarding network and information security.

Under the first pillar, each Member State is required to establish competent authorities for network and information security, which are responsible for monitoring the application of its provisions in sectors falling within its scope. Due to differences in national management structures, Member States may designate more than one national competent authority responsible for performing cybersecurity tasks of key service operators and digital service providers.

In the above context, new obligations of the so-called: key service operators should be looked at. "Key service" means a service that is critical to maintaining critical social or economic activities as listed in the list of key services. The operator of the key service is the entity referred to in Annex No. 1 to the Act on the national cybersecurity system, having an organizational unit on the territory of the Republic of Poland, towards which the authority competent for cybersecurity issues made a decision regarding the recognition of the key service operator. Sectors, subsectors and types of entities are set out in Annex 1 to the Act. The competent authority for cybersecurity makes a decision on the recognition of an entity as a key service operator, if: 1) the entity provides the key service; 2) the provision of this service depends on information systems; 3) the incident would have a significant disruptive effect on the provision of the key service by that operator.

The subjective scope of the directive has been formulated in two formulas: operators of key services and digital service providers. Different requirements apply to the operators indicated in each of the annexes. For digital service providers (Annex III), a gentle and reactive approach is required to cover ex-post supervisory activities, i.e. after the incident and only by the country where the service provider is located. Thus, entities from Annex III will not be subject to the previously described identification or reporting process, as in the case of key service operators. This approach is due to the international dimension of operators providing digital services, and thus the fear of fragmentation of the EU digital single market. As a result of negotiations, it was agreed that

regulations would cover shopping websites, search engines and cloud services. The annex to the Act contains all potential categories of entities in individual sectors of the economy and the state's activity, from which operators of key services can be selected by administrative decision.

In Poland, the Act on the national cybersecurity system has assigned specific tasks to existing entities that deal with computer incident response as part of their activities.

CERT GOV

The Governmental Computer Incident Response Team CERT.GOV.PL acts as the main CERT team responsible for coordinating the process of responding to computer incidents occurring in the area ofgovernment administration and critical infrastructure. One of its basic tasks is recognizing, preventing and detecting threats to security – important from the point of view of the continuity of the state's functioning – ICT systems of public administration bodies or the ICT network system covered by a uniform list of objects, installations, devices and services included in the critical infrastructure, and also ICT systems of owners and holders of critical infrastructure facilities, installations or devices referred to in art. 5b paragraph 7 point 1 of the Crisis Management Act.

RON SRNIK

The Computer Defense Incident Response System of the Ministry of National Defense carries out tasks in coordinating the processes of preventing, detecting and responding to computer incidents in the ICT systems and networks of the Ministry of National Defense.

SRnIK RON is organized into a three-level structure in accordance with NATO assumptions (SRnIK Coordination Center, SRnIK Support Center, which carries out tasks in accordance with the scope of activities of the CERT Teams, and administrators of IT systems of RON units and organizational units).

The main tasks of SRnIK include coordination of response to computer incidents, handling and analysis of events and incidents, as well as conducting activities aimed at increasing awareness of ICT security.

As part of its tasks, SRnIK cooperates with organizational units and units of the Ministry of National Defense, as well as with non-departmental, national and international organizations.

National Center of Cybersecurity

In July 2016, the National Cybersecurity Center (NC Cyber) was established as part of NASK, designed as a center for rapid response to threats and reported incidents in cyberspace, and in the event of possible attacks – to take necessary actions in cooperation with centers in the country and abroad to analyze the nature, manner, extent of the incident, and to exchange information to alert key sectors and institutions. NC Cyber issues recommendations on how to deal with the threat and necessary actions to minimize the effects.

Public and private entities may cooperate with NC of Cybersecurity on the basis of signed agreements in the field of cybersecurity, they may also delegate their representatives to ongoing cooperation.

The Act sets out obligations for operators of key services regarding the implementation of an effective safety management system, including risk management, procedures and mechanisms for reporting and handling incidents or organization of structures at the operator level. In addition, the Act specifies the obligations imposed on digital service providers, taking into account the existing restrictions in this respect set out in Directive 2016/1148. First of all, it is assumed to define CSIRT tasks responsible for counteracting cybersecurity threats of cross-sectoral and cross-border nature, as well as to coordinate the handling of serious, significant and critical incidents. Secondly, the Act provides for the inclusion of cybersecurity aspects in the sphere of state management. In addition, the Act provides for the establishment of the Critical Incident Team as an auxiliary body appointed in the matters of service and coordination of the listed critical incidents at the national level of CSIRT and RCB.

The need for cross-sectoral cooperation results from the fact that the process of emergence of threats is continuous, therefore the list of incident response needs is constantly increasing and thus the list of entities responsible for cybersecurity is expanding. The right selection of legal instruments must meet these needs without negating the classic means. Digital democracy is a form of government activity in which public authorities and public administration bodies are required to counteract any negative trends for

national security. However, it is important to stress the importance of NGOs in activities related to ensuring constantly growing cybersecurity.

Technological changes have also affected the scope of responsibility for criminal acts, but at the same time new rules have emerged related to the limitations of this responsibility. In the European law, the liability of online service providers is regulated by Directive 2000/31 / EC. This directive includes provisions related to the most popular network services: mere conduit, caching and hosting. It should be emphasized here that European regulation adopts a horizontal model. This means that the exclusions it provides apply to all legal liability, including civil, criminal and administrative liability. The e-commerce directive creates rules for exclusion of liability at the maximum level. Therefore, individual Member States may decide to introduce less restrictive solutions.

The implementation of the provisions of the Directive on electronic commerce in Polish law are art. 12–15 of Act on Provision of electronic services. In accordance with art. 12 of this Act, referring to the mere conduit service, if the person who by transmitting data: 1) is not the initiator of the transmission, 2) does not select the recipient of the data and 3) does not delete or modify the data being the subject of transmission, is not responsible for the information provided. The exclusion of liability referred to in paragraph 1 also includes the automatic short-term intermediate storage of transmitted data, if this action is only intended to carry out the transmission and the data is not stored longer than is normally necessary to carry out the transmission (caching, art. 12 section 2 of the Act on Provision of electronic services).

Therefore, respecting the integrity of stored data remains a necessary condition to avoid legal liability. In accordance with art. 13 section 2 of the Act on Provision of electronic services one shall not be liable for stored data who, under the conditions referred to in paragraph 1, immediately deletes the data or prevents the access to the stored data, when he receives a message that the data has been deleted from the initial transmission source or access to them has been prevented, or if the court or other competent authority ordered the deletion of data or preventing access to them, storage of data by the recipient, he is not aware of the unlawful nature of the data or related activities, and in the event of receiving official notification or obtaining reliable information about the unlawful nature of the data or related activities will immediately prevent access to this data.

In turn, Article 14 of Directive 2000/31 / EC should be interpreted as meaning that the rule laid down therein applies to the entity providing the

internet referencing service if, when providing its services, the service provider does not play an active role which could cause him to have knowledge of stored information or have control over it. If the said service provider does not play such a role, he cannot be held liable for the content of information stored at the advertiser's request, unless, having become aware of the unlawful nature of this information or the advertiser's activity, he has not immediately taken appropriate action to remove the said information or prevent access to it .

The regulations listed here justify the thesis that in each case the responsibility of the same entity will be different depending on whether it conducts service activities referred to in the Act on the provision of electronic services, or is the sender or publisher. As a result of technological and economic convergence, the same entity can perform very different functions and it is not a foregone conclusion that its status, and thus the scope of responsibility, is finally established. This situation indicates the need to introduce appropriate regulations, subject to the need to synchronize issues at every stage of substantive legislative activities. This is an essential element in creating a coherent system of regulatory frameworks.

The document Cyberspace Protection Policy of the Republic of Poland states that cyberspace security is a set of organizational and legal, technical, physical and educational projects aimed at ensuring smooth functioning of cyberspace. In turn, a cyberattack is a deliberate disruption of the proper functioning of cyberspace, and cybercrime is a criminal act committed in the area of cyberspace[30]. These definitions were developed on the basis of actions to be taken in the digital domain. Thus, cybercrime is defined as a type of crime in which a computer is either a tool or an object of crime. This term covers all types of crimes that were committed with the participation of a computer or ICT networks or which were directed at these devices. However, the computer can also be the culprit. Therefore, the third area that requires a separate and expanded analysis of the responsibility associated with the functioning of cyberspace is the zone of computer operation. In 1997, Garri Kasparow, one of the world's greatest chess players, lost the game to the Deep Blue program – a specialized supercomputer programmed by IBM and constructed for the price of $ 10 million.

30 Online <file:///C:/Users/kjentkiewicz/Downloads/Polityka_Ochrony_Cyberprzestrzeni_RP_148x210_wersja_pl.pdf>, s. 5, MAiC ABW.

The ability of computers to analyze and solve problems, also in the area of ethics, creates interesting issues regarding the answer to the questions, what is moral and what is immoral, what is good and what is evil, what is allowed and what should be banned in legal approach. These dilemmas are a basic element in determining the degree of responsibility. If we assume that computers are increasingly independent in thinking and decision-making, can it be assumed that they are also aware of the existence of morality? Can the concept of morality be considered by the machine and do computers have morality and is it imposed or their own? This seems to be the key to answering questions related to responsibility for cyberspace activities. The courts try to attribute responsibility for damages caused to people by artificial intelligence machines. Does artificial intelligence have any legal entity or does it have the capacity to perform legal acts? Can computers be responsible for their actions? It seems to be a matter of having legal entity. In various positions of law theorists, such as, for example, Ugo Pagallo, the author of The Law of Robots, proves that we should distinguish between the behavior of robots as tools for interpersonal interaction and as entities in the legal sphere.

It seems a matter of time for an artificial intelligence-led computer to be responsible for the caused damage. Judge Curtis Karnow proposes the creation of a legal entity which he describes as "electronic personality". Although the producers of artificial intelligence will escape the responsibility for its actions after manufacturing the robot, it seems that they will still be responsible under the warranty. The legal doctrine of cyber responsibility will be particularly important in the face of changes in life, in the conditions of the development of artificial intelligence. Today, the principles of responsibility are also defined by the distinction between hardware and software, also in the sphere of law. The potential danger posed by artificially intelligent machines increases when they become mobile. Designing technologies or techniques of artificial intelligence and cyborgs will be important in creating a future in which artificial intelligence will loyally and ethically work for a human being. Of course, the law can always regulate the issues of criminal or civil liability for misconduct, prohibited acts, but the dynamics of the development of artificial intelligence and robotics far exceed the possibilities of regulators and legislators. Under these circumstances, ethical principles and morals dictated by public morals will still be heard.

The concept of online security or cyber security consists of resources protection – data, information, digital content in general, the protection of ICT networks and the protection of content transmission via the network, and

thus the communication process itself. From the specifics of the operation of the network it follows – if we theoretically assume that antivirus software and firewalls do their job – that, like a virus vaccine, they will not work in the event of new threats or modifications of those already known.

Therefore, the process of regulating cyberspace is a multi-stage task, requiring constant monitoring of various socially adverse effects. This also applies to the functioning of machines.

To sum up, it should be noted that today the chess master is not a human or a machine, but a team of people and computers. Computers are still performing activities that they have been programmed for but they lack intuition and creativity. Fortunately, people are strong in what computers are weak at, and this creates a potential partnership.

As Freeman Dyson (1988) said: "technology is God's gift. This is probably the greatest gift after a gift of life. She is the mother of civilization, arts and sciences".

Bibliography

Literature

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 244.

Barta J., Markiewicz R., *Wstęp* [w:] J. Barta, R. Markiewicz (red.), *Handel elektroniczny. Problemy prawne*, Kraków 2005.

Chałubińska-Jentkiewicz K., *Cyberprzestępczość jako paradygmat pojęcia bezpieczeństwa w cyberprzestrzeni*, „Wojskowy Przegląd Prawniczy" 2016, nr 3.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii*, Warszawa 2015.

Goban-Klas T., *Cywilizacja medialna*, Warszawa 2005.

Grzelak M., Lidel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22.

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011.

Siwicki M., *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno-karne*, Warszawa 2011.

Suchorzewska A., *Ochrona prawna systemówin formatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2012.

Legal acts

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. nr 156, poz. 1301).

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. nr 113, poz. 985).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

Odpowiedzialność w sieci – wstęp do problematyki

Streszczenie

Artykuł odnosi się do diagnozy obecnego stanu prawnego w przedmiocie odpowiedzialności w obszarze cyberprzestrzeni, który sam w sobie jest trudny do zdefiniowania. Polskie rozwiązania ustawowe, strategiczne i programowe przygotowywane są w warunkach standardów UE. Analiza obejmuje przegląd zagrożeń (głównie związanych z infrastrukturą informacyjną i teleinformatyczną) i ich uwarunkowań (systemowych, ekonomicznych, społeczno-kulturowych). Istotną kwestią jest ustalenie adresatów zobowiązanych do działań zapobiegawczych i eliminacyjnych (przede wszystkim władz publicznych, ale także innych, np. podmiotów komercyjnych lub przedstawicieli działających na rynku społeczeństwa informacyjnego). Odpowiedzialność za działania w sieci dotyczy także kwestii współpracy merytorycznej i instytucjonalnej na poziomie europejskim.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, odpowiedzialność, zagrożenia, społeczeństwo informacyjne, infrastruktura informacyjna, infrastruktura teleinformatyczna, komunikacja, nowe technologie

Piotr Grochmalski*

Nowy paradygmat bezpieczeństwa a AI**

Streszczenie

Artykuł dotyczy zagadnień implikacji rozwoju AI dla zmian paradygmatu bezpieczeństwa, dotychczas posiadającego w swej istocie ontyczny, antropocentryczny wymiar, chociaż wpisany w szerszy kontekst społecznych badań nad postępem i nowoczesnością, oraz wynikających z nich zagrożeń. Warunkowane technologicznie zmiany struktur społecznych zwiększają ryzyko dla ludzkości, zwłaszcza jeśli uwzględnić problem tzw. punktu bifurkacji, w którym układ nierównowagowy jest w momencie krytycznym, a nadal nie stworzono ogólnej teorii opisującej złożoność. Obecnie podstawowym celem nauk o bezpieczeństwie winno być zatem zabezpieczanie ontycznego istnienia ludzkości wobec wyzwań i nowej logiki zagrożeń ze strony super inteligentnej AI.

Słowa kluczowe: bezpieczeństwo, superinteligencja, technologia, zagrożenie, sztuczna inteligencja, społeczeństwo, globalizm.

* Dr hab. prof. nadzw. Piotr Grochmalski, dyrektor Instytutu Studiów Strategicznych, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej, e-mail: p.grochmalski@akademia.mil.pl.

** Artificial intelligence (AI).

Czy nasz gatunek jest „mądry"? – pyta prowokacyjnie Michał Heller w rozprawie *Moralność myślenia*[1]. 13 czerwca 2018 r. Sophia – humanoidalny robot wyposażony w elementy sztucznej inteligencji, dzieło firmy Hanson Robotics z Hongkongu – odebrała indeks Akademii Górniczo-Hutniczej w Krakowie. Był to element promocji tej uczelni, który jednak stworzył szereg problemów. Jak prawnie interpretować to wydarzenie? Jak wobec tego określać relacje student–nauczyciel? Kim czy raczej czym jest Sophia? W październiku 2017 r. robot ten otrzymał obywatelstwo Arabii Saudyjskiej. Tworzymy fakty, nie pojmując ich długofalowych konsekwencji.

***

Każdy akt ludzki (łac. *actus humanus*) ma swe elementarne źródło w rozumowym poznaniu otoczenia i w wolnej woli istoty ludzkiej. Jest on nieodłączną częścią naszego człowieczeństwa. Wraz z rozwojem struktur społecznych człowiek, poprzez swoje akty woli, stara się realizować rozpoznawane i powstające potrzeby. Istnieje daleko idąca zbieżność poglądów, iż jedną z naturalnych potrzeb człowieka jest potrzeba bezpieczeństwa. Zgodnie z zasadą antropiczną[2], będącą w istocie rodzajem dyrektywy o charakterze epistemologicznym, z faktu istnienia człowieka we wszechświecie można wyprowadzić szerszą wiedzę na temat właściwości tego wszechświata. To podejście pozwala głębiej wniknąć w rodzaj powiązań między światem organicznym i nieorganicznym pozwalających na powstanie życia i jego ewolucję.

Przy całym zróżnicowaniu badań nad bezpieczeństwem fundamentalnie tkwią one w założonym implicite paradygmacie, że ogniskują się wokół człowieka i wszelkich form ludzkich wspólnot. Klarownie ujmuje to Waldemar Kitler, gdy zauważa, iż „Wszelkie analizy bezpieczeństwa (…) muszą się odbywać przynajmniej z określeniem jego rodzaju, a w konsekwencji jego podmiotu i przedmiotu. Bez wątpienia we wszelkich rozważaniach o bezpieczeństwie jego podmiotem jest zawsze człowiek, którego pewność wolności od zagrożeń oraz niezakłóconego bytu i rozwoju wiąże się z wielopoziomowymi i wielowarstwowymi sposobami zabezpieczenia potrzeb w tym zakresie"[3]. Obowiązujący paradygmat nauk o bezpieczeństwie w swoim podstawowym wymiarze ma

1 Tak brzmi tytuł pierwszego podrozdziału w rozdziale 6. *Kręte drogi rozumu* – patrz: M. Heller, *Moralność myślenia*, Kraków 2017, s. 103.

2 Zasadę antropiczną wprowadził do nauki B. Carter; szerzej – patrz: *Słownik filozoficzny*, t. 1, s. 243–246.

3 W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011, s. 23–24.

charakter ontyczny, jest antropocentryczny – skupia się na bezpieczeństwie człowieka i społeczeństwa, a szerzej – ludzkości. A jednak świat się zmienia, a wraz z nim granice jego interpretacji i interpretacji naszego w nim miejsca. Bartosz Brożek twierdzi, iż „Zmiany w obrazie świata – szczególnie w centralnej jego części – nie mogą być natychmiastowe. Jest to zwykle długi ewolucyjny proces, a nie jednorazowa rewolucja"[4]. Ewolucja granic interpretacji stawia problem tzw. punktu bifurkacji, w którym układ nierównowagowy jest w punkcie krytycznym. „Najmniejsze przypadkowe wahanie może przechylić szalę i nieodwołalnie określić przyszły los układu"[5]. Sytuacja ta odnosi się do obszaru fizyki dotyczącego termodynamiki nierównowagowej. Nie można jej wprost transponować do rzeczywistości społecznej, ale dobrze opisuje cechy zbioru, który charakteryzuje się dużą złożonością. Manuel Castells w trzech publikacjach, które stanowią zwarty opis dokonujących się procesów transformacji i modernizacji we współczesnym świecie (*Społeczeństwo sieci*[6], *Siła tożsamości*[7], *Koniec tysiąclecia*[8]), wskazuje, iż w coraz większym stopniu, pod wpływem technologii, głębokim przekształceniom uległy nasze struktury społeczne. internet, sztuczne sieci neuronowe, algorytmy, uczenie maszynowe, nanotechnologie formatują i narzucają nam nowe formy społecznej i osobistej aktywności. Stajemy przed wyzwaniami kreowanymi przez naukę i technologie, które mogą mieć charakter układu nierównowagowego zbliżającego się do punktu krytycznego. Nadal nie stworzono ogólnej teorii opisującej złożoność[9]. Rozpoznano jednak w ostatnich latach strukturę o typie złożoności, która zaintrygowała badaczy. Nazwano ją samozorganizowanym stanem krytycznym (*self-organizing critically*, SoC)[10]. Internet, wyposażony w quasi-inteligentne algorytmy, może ulegać takiej strukturalnej formie krytycznej samoorganizacji i zmierzać do tzw. punktu bifurkacji w relacji ze społeczeństwem.

Jako ludzkość od drugiej połowy XX w. posiedliśmy środki wystarczające dla wywołania globalnej katastrofy. John D. Barrow uważa, iż „kultury naukowe, w rodzaju naszej własnej, muszą zawierać w sobie ziarna własnej destrukcji"[11]. Ten angielski fizyk i matematyk zauważa, iż „Skłonność do krótkotermi-

4 B. Brożek, *Granice interpretacji*, Kraków 2018, s. 233.
5 P. Ball, *Masa krytyczna. Jak jedno z drugiego wynika*, Kraków 2007, s. 141.
6 M. Castells, *Społeczeństwo sieci*, Warszawa 2008.
7 M. Castells, *Siła tożsamości*, Warszawa 2008.
8 M. Castells, *Koniec tysiąclecia*, Warszawa 2009.
9 J.D. Barrow, *Kres możliwości? Granice poznania i poznanie granic*, Opole 2005, s. 163.
10 Ibidem.
11 Ibidem, s. 135.

nowych korzyści zamiast do ultra długoterminowego planowania nie pozwoli nam powstrzymać katastrof, które powoli i stopniowo stają się coraz bardziej realne, choć niezauważalne w ciągu jednego ludzkiego życia"[12]. Ryzyko potencjalnej katastrofy ludzkości zdaje się wpisane w cywilizacyjny rozwój, który coraz bardziej przyspiesza. Ray Kurzweil zauważa: „w XXI wieku będziemy świadkami nie stu lat postępu technologicznego, ale postępu rzędu 20 tys. lat (oczywiście w stosunku do dzisiejszej szybkości postępu) lub tysiąc razy większego niż ten osiągnięty w XX wieku[13]". Będzie się pogłębiało zjawisko „odklejania się" czasu społecznego od technologicznego. Ta dysharmonia będzie wywoływać rosnącą presję na poszukiwanie technicznych narzędzi do jej przezwyciężania. Ale dystans będzie logarytmicznie rósł, a nie malał. W ciągu ludzkiego życia będą umierać kolejne „pokolenia" technologii, a ich czas trwania będzie się radykalnie skracał.

Przyjmujemy, iż nauki o bezpieczeństwie miały charakter zasadniczo utylitarny i ewoluowały w zależności od definiowania i postrzegania zagrożeń, zaufania i ryzyka. Są one wpisane w szerszy kontekst społecznych badań nad postępem i nowoczesnością oraz wynikających z nich zagrożeń (Anthony Giddens mówi o ciemnej stronie nowoczesności)[14]. Maciej Żukowski w przedmowie do polskiego wydania dzieła Raya Kurzweila *When humans transcend biology* zauważa, iż: „…moc obliczeniowa maszyn podąża od ponad 100 lat dość przewidywalną ścieżką podwajania swojej wartości w ciągu każdych 18–22 miesięcy. Jeśli następne lata nie przyniosą załamania tej tendencji, to we wczesnych latach 20. naszego stulecia moc obliczeniowa komputera wartego 1000 USD będzie zbliżona do mocy ludzkiego mózgu. Ten sam komputer 15–20 lat później będzie dysponował mocą wszystkich ludzkich mózgów! Na naszych oczach odbywa się cicha rewolucja, której przyszłe skutki zdaje się zauważać bardzo niewielu, ale której konsekwencje dotkną każdego na tej planecie. (…) Dominować zacznie inteligencja niebiologiczna, która będzie wielokrotnie potężniejsza od ludzkiej, a także, co bardziej zdumiewające, której tempo rozwoju będzie stale przyspieszało, zgodnie z wykładniczym charakterem całego procesu"[15]. Ray Kurzweil, jeden z najwybitniejszych teoretyków i praktyków zajmujących się AI, a przy tym główny autorytet w środowisku transhumani-

12 Ibidem.
13 R. Kurzweil, *Nadchodzi osobliwość*, Warszawa 2013, s. 26.
14 A. Giddens, *Konsekwencje nowoczesności*, Kraków 2008, s. 5.
15 M. Żukowski, Przedmowa do wydania polskiego [w:] R. Kurzweil, *Nadchodzi osobliwość*, Warszawa 2013, s. 13–14.

stów, uważa, iż efektem rozwoju sztucznej inteligencji będzie proces postępującej integracji człowieka z maszyną, w wyniku której powstanie nowa forma integracji istoty biologicznej zbytem cyfrowym. Nick Bostrom, kierownik Instytutu Przyszłości Ludzkości działającego przy Oxford Martin School, nie podziela optymizmu Kurzweila. Uważa, iż naturalną konsekwencją stworzenia przez człowieka sztucznej inteligencji będzie jej dalszy rozwój, aż do momentu, gdy radykalnie stanie się inteligentniejsza od całej ludzkości. Po przekroczeniu punktu krytycznego może uzyskać ona nad nami strategiczną przewagę, której najprawomocniej nie utraci. Bostrom wprowadził do dyskursu naukowego pojęcie superinteligencji. W jego ujęciu to dowolny umysł mający wielokrotnie większe zdolności poznawcze i kreatywne w dowolnym obszarze aktywności od globalnego potencjału wszystkich umysłów ludzi. Oba stanowiska wskazują jednak, iż zbliżamy się do owego punktu bifurkacji dla rozwoju badań nad AI, a to oznaczać winno, iż obecny paradygmat bezpieczeństwa winien ulec zmianie – podstawowym celem nauk o bezpieczeństwie winno być zabezpieczanie ontycznego istnienia ludzkości wobec wyzwań i zagrożeń ze strony super inteligentnej AI.

Nie jesteśmy w stanie stwierdzić, na ile wizje pokroju Kurzweila i Bostroma trafnie prognozują kierunki rozwoju ludzkości. Przyjrzymy się jednak kilku wybranym aspektom współczesnego świata, by spróbować odpowiedzieć na pytanie, czy powstaje potencjał krytyczny, który może przesądzić o naszej przyszłości. Rozważmy kilka procesów, które będą wpływały na konieczność zmiany paradygmatu bezpieczeństwa: 1) wykładniczy przyrost liczby algorytmów mających cząstkowe cechy AI (rewolucja AI); 2) infrastrukturalny globalny projekt danetyzowania świata; 3) ontyczna rewolucja prawa – załamanie antropocentryzmu w prawie; 4) globalny wyścig w dziedzinie sztucznej inteligencji.

Wykładniczy przyrost liczby algorytmów mających cząstkowe cechy AI (rewolucja AI)

W 1936 r. Alan Turing napisał pracę *O liczbach obliczalnych z zastosowaniem do problemu wyboru* (ang. *On Computable Numbers with an Application to the Entscheidungsproblem*), w której przedstawił założenia hipotetycznej idealnej maszyny liczącej. Był to jedynie myślowy eksperyment, który stał się podstawą

stworzenia komputera[16]. „Zdefiniował też obliczanie jako mechaniczną procedurę, algorytm"[17]. W 1950 r. wymyślił test inteligencji dla maszyny. Jednak teoretyczne fundamenty pod skonstruowanie podstaw współczesnej infosfery stworzyła praca Claude'a Elwooda Shannona (1916–2001) *A Mathematical Theory of Communication* opublikowana w 1948 r. (w 55-stronicowym artykule ten amerykański matematyk wprowadził m.in. bit jako jednostkę najmniejszej ilości informacji)[18]. Sam Shannon miał świadomość fundamentalnej słabości swej teorii – rzecz dotyczyła niemożliwości wytłumaczenia istotności informacji – liczyła się „masa" binarna, a nie jej wartość poznawcza. Pojęcie prawdy w jej wymiarze etycznym zanika, a jej miejsce zastąpione jest przez „atom" informacji. W takim wymiarze znika aksjologia jako nieprzekładalna na język binarny, a jej miejsce zajmuje to, co może być zredukowane i zapisane za pomocą dwóch stanów lub cyfr 0 i 1. Pięć lat później John McCarthy użył pojęcia *artificial intelligence* na określenie maszyn, które przejawiałyby cechy ludzkiej inteligencji. W tym samym roku Arthur Samuel zaprezentował, udoskonalony o mechanizmy uczenia maszynowego, program szachowy. Był to pierwszy program, który pokonał w grze swojego twórcę[19]. W 1956 r. kilkunastu badaczy, których pochłaniały badania nad maszynową inteligencją, w tym głównie John McCarthy, Marvin Minsky, Nathaniel Rochester i Claude Shannon, spotkało się w Dartmouth College na sześciotygodniowych warsztatach[20]. Ten moment uznaje się za początek profesjonalnych badań nad AI.

Po siedmiu dekadach od tych wydarzeń złożone algorytmy są nieodłącznym tłem naszego codziennego życia – są nie tylko w telefonach, komputerach, laptopach, ale w samochodach, sprzęcie AGD, biurach, urzędach. Wydarzeniem szeroko komentowanym w świecie była przegrana w 1997 r. Garriego Kasparowa, szachowego mistrza świata, z programem komputerowym Deep Blue firmy IBM. Dwanaście lat po tym wydarzeniu, w 2009 r. program Pocket Fritz 4, zamontowany w telefonie mobilnym HTC Touch, wygrał turniej mistrzowski Copa Mercosur w Buenos Aires w Argentynie (9 zwycięstw i jeden remis)[21]. Fakt ten pokazuje skalę postępu, jaki nastąpił w maszynowych sys-

16 J. Gleick, *Informacja. Bit. Wszechświat. Rewolucja*, Kraków 2012, s. 190–191.
17 Ibidem, s. 192.
18 C.E. Shannon, *A Mathematicval Theory of Communication*, online <http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf>.
19 N. Bostrom, *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016, s. 32.
20 T. Walsh, *To żyje. Sztuczna inteligencja. Od logicznego fortepiano po zabójcze roboty*", Warszawa 2018, s. 32–33.
21 Ibidem, s. 99.

temach uczących się. Do niedawna główny wysiłek skupiony był na rozwoju technik probabilistycznych w ramach wnioskowań bayesowskich czy też wektorów nośnych. Jednak jakościowy skok nastąpił w wyniku zastosowania sztucznych sieci neuronowych. W 2013 r. niewielka firma Deep Mind, stosując tę technologię, „nauczyła" maszyny gry w szereg klasycznych gier komputerowych. „W większości przypadków komputery potrafiły grać na poziomie człowieka. W kilkunastu przypadkach grały na poziomie superludzkim. Był to zadziwiający wynik, gdyż program nie otrzymał żadnej wstępnej wiedzy o tych grach. Miał tylko dostęp do wyników i pikseli na ekranie. Nauczył się każdej z gier od zera"[22]. Technologia deep learning jest tym skuteczniejsza, im szerszy ma dostęp do dużych baz danych. Jesteśmy we wstępnej fazie rozwoju internetu rzeczy (*Internet of Things*, IoT). Jego błyskawiczny rozwój stworzy doskonałe środowisko do szybkiego rozwoju potencjału tej technologii. Wydarzeniem, które pokazało potencjał współczesnych algorytmów, było pokonanie w 2011 r. przez komputer Watson firmy IBM ludzi, którzy brali udział w popularnym amerykańskim teleturnieju *Jeopardy*. Do konfrontacji z maszyną wybrano najlepszych graczy w historii tej gry. W tej swoistej rywalizacji człowieka z maszynami trudno znaleźć obecnie gry logiczne, w których jesteśmy w stanie rywalizować z komputerami. W 2006 r. program Quackle okazał się lepszy od Davida Boysa, byłego mistrza świata w scrabble[23]. W 2017 r. boty pokerowe Liberatus z CMU i Deep Strack opracowany przez zespół czesko-kanadyjski wygrały ze światową czołówką w grze w pokera[24]. Przegrywamy także w gry, które – jak sądziliśmy dotąd– wymagają od ich uczestników szczególnych zdolności i intuicji.

Świat piękna, tworzenie dzieł sztuki miały być wyłączną domeną ludzkiej aktywności. Zdolność do tworzenia piękna uznawaliśmy za jedną z konstytutywnych naszych cech. Także ten element naszego człowieczeństwa staje się obszarem, na który wkraczają algorytmy. W dniu 25 października 2018 r. dom aukcyjny Christie's wystawił na licytację i sprzedał za 425,5 tys. dolarów grafikę stworzoną przez algorytm. Współtwórca programu Hugo Caselles-Dupré tak wyjaśniał swoją motywację: „We found that portraits provided the best way to illustrate our point, which is that algorithms are able to emulate creativity"[25]. Równie dynamicznie algorytmy wkraczają w przestrzeń medialną.

22 Ibidem, s. 47.
23 Ibidem, s. 103.
24 Ibidem.
25 „Stwierdziliśmy, że portrety są najlepszym sposobem zilustrowania naszego punktu, a mianowicie, że algorytmy są w stanie naśladować kreatywność" (tłum wł.) – patrz:

Chińska firma Turing Robot stworzyła bota o nazwie Baby Q, który poprzez rozmowy z ludźmi w sieci miał rozwijać swoje zdolności konwersacyjne (został wyłączony, gdy zaczął się wypowiadać negatywnie o Komunistycznej Partii Chin)[26]. Z kolei chińska agencja rządowa Xinhua w 2018 r. rozpoczęła wykorzystywać bota jako sztucznego prezentera w kanale informacyjnym[27].

Algorytmy wykorzystywane są we współczesnych systemach rozpoznawania mowy opartych np. na ukrytych modelach Markowa. Dzięki takim rozwiązaniom osobiści asystenci cyfrowi – np. Siri firmy Apple, w który został wyposażony IPhon 4S wypuszczony na rynek w 2011 r., są stałym elementem naszej rzeczywistości. Coraz więcej mobilnych urządzeń wyposażonych jest w systemy rozpoznawania znaków (*Optical Character Recognition*, OCR). Wyszukiwarki stają się coraz bardziej złożonymi programami. Algorytm Hummingbird, zdolny do semantycznej analizy zapytań, który Google wprowadził do swej wyszukiwarki w 2013 r., bierze pod uwagę całą frazę pytania, a także swoją „wiedzę" na temat wcześniejszych wyszukiwań danej osoby, porę dokonywanej operacji, a nawet jej lokalizację[28]. Jeden z najważniejszych w wyszukiwarce Google algorytm Panda, wdrożony w 2012 r., w ciągu pierwszych dwóch lat funkcjonowania był 24 razy modyfikowany[29]. W 2010 r. Google ogłosił na swoim blogu, że w pełni bezobsługowe auta jeżdżą już od pewnego czasu po amerykańskich drogach[30]. Następuje też ingerencja algorytmów wprost w struktury biologiczne naszego ciała. W 2017 r. Lee Organick, Karl Koscher i Peter Ney z Uniwersytetu stanowego Waszyngton w Seatle udanie wszczepili w próbkę DNA złośliwe oprogramowanie. W ten sposób zainfekowali komputer, który analizował tę próbkę DNA, a następnie przejęli nad nim kontrolę[31].

Is artificial intelligence set to become art's next medium?, online <https://www.christies.com/features/A-collaboration-between-two-artists-one-human-one-a-machine-9332-1.aspx.

26 *Kochasz partię komunistyczną? „Nie". Chiński bot znika z sieci za krytykę rządzących*, online <https://www.tvn24.pl/wiadomosci-ze-swiata,2/chiny-bot-ze-sztuczna-inteligencja-znika-z-sieci-za-krytyke-partii,761745.html>.

27 S. Czubkowska, *AI zamiast prezentera w chińskiej agencji prasowej*, wyborcza.pl, online <http://wyborcza.pl/7,156282,24143179,ai-zamiast-prezentera-w-chinskiej-agencji-prasowej-wyglada.html>.

28 E. Enge, S. Spencer, J.C. Stricchiola, *SEO, czyli sztuka optymalizacji witryn dla wyszukiwarek*, Gliwice 2016, s. 146.

29 Ibidem, s. 540–541.

30 E. Brynjolfsson, A. Mcafee, *Drugi wiek maszyn. Praca, postęp i dobrobyt w czasach genialnych technologii*, Warszawa 2015, s. 32.

31 *Computer Security and Privacy in DNA Sequencing*, online <http://dnasec.cs.washington.edu/>.

Powstają też zwarte, rozbudowane systemy, które przy użyciu rozbudowanej struktury algorytmów mają modelować lub nadzorować całe grupy społeczne, a nawet narody. Rząd ChRL jest w trakcie wdrażania narodowego systemu reputacji (*citizen scoring*), który ma tworzyć rating obywateli w oparciu o te społeczne zachowania, które są utrwalane w ramach ich sieciowej aktywności. Algorytmiczny system reputacji będzie określał naszą szansę na dalszą karierę i rozwój personalny. Przed pełną aktywizacją programu poddano go próbie pilotażowej w ośmiu różnych wariantach. Jak zauważają analitycy z Centrum Badań nad Bezpieczeństwem Akademii Sztuki Wojennej, „Chiński system ratingu obywatelskiego należy uznać za eksperyment społeczny na ogromną skalę. Nie jest zrozumiałe, jakie dokładnie korzyści władze chcą uzyskać dzięki silniejszej regulacji zachowań i działań swoich obywateli”[32]. Elementem tego przedsięwzięcia będzie systemem rozpoznawania twarzy – algorytm AI ma oceniać zachowanie osób i ryzyko popełnienia przez nie przestępstw.

Infrastrukturalny globalny projekt danetyzowania świata

Algorytmy poruszają się w coraz bardziej zagęszczającym się środowisku informacji. Jesteśmy w początkowym stadium rewolucji big data. Tworzy się nowa, realna, interaktywna rzeczywistość oparta na internecie rzeczy. Według szacunków Instytutu Badawczego Gartner już w 2020 r. IoT obejmie 26 mld urządzeń, a International Data Corporation (IDC) ocenia, iż będzie ich aż 212 mld[33]. Zalew danych wymusi szybki rozwój narzędzi uczenia maszynowego. Tempo przyrostu danych dobrze oddaje projekt realizowany od 2000 r., który dotyczył obserwacji nieba w oparciu o projekt *Sloan Digital Sky Survey*. Teleskopy, które wykorzystano do tego programu, w ciągu kilku tygodni zebrały tyle danych, ile dotąd zgromadzono w historii astronomii[34]. Martin Hilbert określił masę binarną zebraną do 2007 r. na 300 eksabajtów (EB) danych[35]. Tempo digitalizacji przyspiesza – jeszcze w 2000 r. tylko czwarta część informacji była

32 *Chiński system zautomatyzowanej oceny obywateli: możliwe konsekwencje wdrożenia* [w:] Ośrodek Studiów nad Wyzwaniami Cywilizacyjnymi – Centrum Badań nad Bezpieczeństwem, Akademia Sztuki Wojennej, Biuletyn nr 4/maj 2017, s. 17.

33 M. Miller, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016, s. 29.

34 V. Mayer-Schönberger, K. Cukier, *Big data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa 2014, s. 21.

35 Ibidem, s. 23.

zgromadzona w formie cyfrowej. Według szacunków w 2013 r. liczba globalnych danych wynosiła 1200 eksabajtów, z czego tylko 2 proc. nie jest zapisanych w formie cyfrowej[36]. Cisco Systems ocenia, że w latach 2006–2011 globalny ruch internetowy wzrósł 12-krotnie, osiągając 23,9 eksabajta miesięcznie[37]. Firma ta prognozuje, iż globalny ruch IP osiągnie 4,8 zettabajta (ZB) w 2022 r. (miesięcznie 396 eksabajtów). W 2017 r. miesięcznie ruch IP osiągał 122 eksabajty, a więc niemal dziesięć razy więcej niż w 2011[38]. Globalny ruch internetowy w 2017 r. osiągnął natężenie porównywalne do informacji zapisanych na 288 mld płyt DVD w ciągu roku (33 mln płyt DVD w ciągu godziny)[39]. Ta logarytmicznie rosnąca ilość danych jest coraz lepszym narzędziem do prognozowania określonych działań. Inżynierowie z koncernu Google przedstawili Flu Trends – narzędzie potrafiące, na podstawie danych gromadzonych przez przeglądarkę, przewidywać z wyprzedzeniem pojawienie się epidemii grypy. Na podstawie analizy 450 milionów modeli matematycznych analitycy koncernu znaleźli kombinacje 45 fraz wyszukiwanych przez ludzi w internecie, które najlepiej pokrywały się z miejscami, gdzie rzeczywiście wystąpiły epidemie grypy[40]. Ogromne bazy danych wykorzystywane są też do profilowania zachowań wyborczych obywateli. Dr Michał Kosiński z Uniwersytetu Stanforda opracował algorytm, który pozwala stworzyć profil psychologiczny człowieka, opierając się na jego aktywności w mediach społecznościowych. Na podstawie 70 do 100 „lajków" z Facebooka algorytm jest w stanie posiąść wiedzę na temat danej osoby porównywalną z tą, jaką dysponuje na jej temat rodzina. Wykorzystując 250 „lajków", uzyskujemy zdolność do przewidywania zachowań danego człowieka większą niż jego współmałżonek. Cambridge Analitica, firma, która posłużyła się tym algorytmem, zebrała 5 tys. danych o każdym z 220 mln wyborców w USA. Miała wykorzystać go w prezydenckiej kampanii wyborczej w USA w 2016 r.[41] Danetyzacja i algorytmizacja zmienia instytucje państwa i całe społeczeństwa. W nieodległej przyszłości miliony

36 Ibidem, s. 24.

37 VNI Forecast Highlights, Cisco, online<www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html>.

38 Ibidem.

39 Ibidem.

40 J. Ginsburg i in., *Detecting Infuelza Epidemics Using Search Engeine Query Data*, „Nature" nr 457, 2009, s. 1012–1014, online <https://www.nature.com/articles/nature07634.

41 J. Karpiński, *To Polak stoi za algorytmem wykorzystywanym przez Cambridge Analitycal. Jego narzędzie pozwala wpływać na wyniki wyborów*, na: Temat, online <https://natemat.pl/233251,kim-jest-michal-kosinski-tworzyl-algorytm-znany-z-cambridge-analytica>.

ludzi na świecie oddadzą kierownice swych aut algorytmom. Bezobsługowe auto Goolge posiada złożony system odbioru i przetwarzania informacji, którego jądrem jest LIDAR wyprodukowany przez firmę Velodyne. Urządzenie to składa się z 64 zintegrowanych laserów, każdy z nich posiada jednak własną autonomię. LIDAR obraca się w tempie 10 obrotów na sekundę, a w ciągu jednej sekundy zbiera 1,3 mln informacji. Na ich bazie komputer tworzy w czasie rzeczywistym dynamiczny obraz całej przestrzeni w promieniu stu metrów od auta[42].Nie ma tu granicy. Wszystko jest informacją i cała przestrzeń może być w nią przekształcona.

Victor Mayer-Schönberger i Kenneth Cukier zauważają, iż proces cyfryzacji przekształcił się w globalne zjawisko danetyzacji. W ich ujęciu „Danetyzacja oznacza zbieranie informacji o wszystkim, wliczając w to kwestie, o których nigdy nie myślelibyśmy jako o źródłach danych, takie jak miejsce przebywania konkretnej osoby, wibracje silnika czy naprężenia występujące w moście, i przetworzone w określony format w celu ich skwantyfikowania"[43]. W ramach projektu danetyzacji firma Google realizuje projekt danetyzacji zasobów drukowanych ludzkości. Według szacunków zespołu kierowanego przez Jeana-Baptiste Michela od wynalezienia druku powstało na świecie 130 milionów książek. Od 2005 do 2012 r. Google zdanetyzowało ponad 20 milionów tytułów[44]. W oparciu o te ogromne zasoby badacze z Harvardu po analizie 500 miliardów słów ustalili, iż mniej niż połowa angielskich wyrazów znajdujących się w tych książkach występowała w słownikach[45]. Ale eksplozja danych obejmie głównie IoT. Będą one wykorzystywane przez maszyny do rozbudowywania infrastruktury informacyjnej, do stopniowej danetyzacji świata. Market Psych wspólnie z agencją informacyjną Thomson Reuters stworzył 18 864 indeksy w 119 krajach świata ukazujące stany emocjonalne ludzi czy zmiany innowacyjne w przestrzeni technologicznej, a także wszelkie istotne konflikty społeczne. Indeksy są aktualizowane co minutę i dostarczane do komputerów, które w oparciu o algorytmy oceniają ryzyko określonych operacji na giełdach[46]. Owa „danetyzacja uczuć i emocji" w procesach analizy kohortowo-behawioralnej big data jest stosowana do przekształcania w informację wszelkich ludzkich uczuć i emocji. W coraz większym stopniu stosuje się ją w nowoczesnych

42 E. Brynjolfsson, A. Mcafee, *Drugi wiek maszyn…*, s. 32.
43 V. Mayer-Schönberger, K. Cukier, *Big data. Rewolucja…*, s. 31.
44 Ibidem.
45 Ibidem, s. 116.
46 V. Mayer-Schönberger, K. Cukier, *Big data. Rewolucja…*, s. 126–127.

technikach targetowania reklam w oparciu o analizę danych użytkowników takich portali, jak Facebook[47]. Michael Miller zauważa, iż „(…) w internecie rzeczy nie chodzi tylko o łączenie ze sobą rzeczy, ale też o autonomiczne działanie rzeczy, które mogą działać same, bez większego udziału człowieka"[48]. Internet rzeczy stopniowo będzie się stawać coraz bardziej autonomiczny od ludzi. W tej chwili „jest w trakcie definiowania samego siebie. Każdego dnia w jego obrębie zachodzą liczne zmiany[49]". Manuel Castells w swoim klasycznym dziele *Społeczeństwo sieci* zauważał, iż już w bliskiej perspektywie elektronika molekularna stworzy nową rzeczywistość digitalną. Bowiem „elektronika molekularna stanowi drogę pokonania fizycznych ograniczeń w zwiększaniu gęstości upakowania tranzystorów krzemowych w chipie. Zapoczątkowałoby to erę komputerów 100 mld razy szybszych od mikroprocesora Pentium: stałoby się możliwe stworzenie urządzenia wielkości ziarenka soli o wydajności stu serwerów komputerowych z 1999 r. Informatycy rysują perspektywę powstania na bazie tych technologii środowiska informacyjnego, w którym miliardy mikroskopijnych urządzeń do przetwarzania informacji będą rozprzestrzenione wszędzie, niczym »pigment w farbie na ścianach«. Sieci komputerowe stałyby się wtedy, w sensie dosłownym, strukturą naszego życia"[50].

Michał Heller uważa, iż: „Niesłychana skuteczność nauki w badaniu świata mówi nam coś o samym świecie: świat ma pewną cechę, dzięki której ulega badaniom naukowym, cechę tę nazywam racjonalnością świata"[51]. Heller wprost stawia tezę o matematyczności przyrody – „przyrodę daje się opisywać matematycznie"[52]. James Gleick uważa, iż wszystko może być zdanetyzowane, także fundamentalne prawa kształtujące naszą fizyczną rzeczywistość: „Gdy zachodzi interakcja między protonami, elektronami i innymi cząsteczkami, co tak naprawdę się dzieje? Następuje wymiana bitów, przekaz stanów kwantowych, przetwarzanie informacji. Prawa fizyki to algorytmy"[53]. Czy to znaczy, że także człowiek może ulec pełnej danetyzacji? W 1913 r. Rober Musil z wielką emfazą opisywał wszechmoc matematyki. Podkreślał wówczas, iż: „Z wyjątkiem

47 D. Dudek, *Jak sprzedać wycieczkę. Danetyzacja uczuć i emocji na przykładzie biur podróży*, online <http://jakrobicmarketing.pl/jak-sprzedac-wycieczke-danetyzacja-uczuc-i-emocji-na-przykladzie-biur-podrozy/>.
48 M. Miller, *Internet rzeczy...*, s. 18.
49 Ibidem, s. 19.
50 M. Castells, *Społeczeństwo sieci*, Warszawa 2008, s. 64–65.
51 M. Heller, *Filozofia i wszechświat*, Kraków 2006, s. 35.
52 Ibidem, s. 11.
53 J. Gleick, *Informacja*, Kraków 2012, s. 16.

niektórych ręcznie wykonywanych mebli, ubrań, butów, a także dzieci, wszystko otrzymujemy przy zastosowaniu obliczeń matematycznych. Wszystko, co biega wokół nas, pędzi lub stoi, jest zależne od matematyki nie tylko dlatego, że bez niej jest niewytłumaczalne, lecz także dzięki niej faktycznie powstało i na niej się opiera w swojej tak a nie inaczej określonej egzystencji”[54]. Dzisiaj zmierzamy coraz szybciej do kwantyfikowania i przekładania wszelkich elementów rzeczywistości na dane, by móc poddać je agregowaniu i algorytmizacji. Ale im precyzyjniej każdy możliwy aspekt egzystencji człowieka zostanie skwantyfikowany i zarejestrowany, tym lepiej będziemy sprofilowani i rozpoznawalni w dowolnym miejscu i czasie w zdanetyzowanej rzeczywistości, która stanie się autonomiczna wobec ludzkości.

Ontyczna rewolucja prawa a perspektywa załamania antropocentryzmu w prawie

Postępująca danetyzacja, algorytmizacja i robotyzacja otoczenia człowieka powoduje, iż coraz częściej w przestrzeni publicznej pojawia się temat praw dla robotów, na wzór praw człowieka. W sprawozdaniu Komisji Europejskiej z 2017 r. nie wyklucza się, że wyjątkowo zaawansowane maszyny mogą się w przyszłości stać „osobami elektronicznymi”[55].

Z kolei indyjski „Report of The Artificial Intelligence Task Force 2018” wprowadza pojęcie „byty autonomiczne”[56]. Autorzy zauważają, iż w bliskiej perspektywie „przyjdzie się nam zmierzyć z pytaniem o prawa i odpowiedzialność bytów autonomicznych”[57]. Ale konkretne wydarzenia już kierunkują przyszłe regulacje prawne w tej mierze. W Tokio bot o imieniu Shibuya Mirai, mający cechy 7-letniego chłopca, ale niemający żadnej „cielesności” uzyskał stałe zameldowanie[58]. Z kolei pod imieniem i nazwiskiem Fran Pepper „żeński”

54 R. Musil, *Człowiek matematyczny i inne eseje*, Warszawa 1995, s. 25–26.

55 Rezolucja Parlamentu Europejskiego z 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL)), Prawo.pl, online <https://www.prawo.pl/akty/dz-u-ue-c-2018-252-239,69072191.html>.

56 *Report of The Artificial Intelligence Task Force 2018*, online <https://dipp.gov.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf>.

57 *Report of The Artificial Intelligence Task Force 2018*,online <https://dipp.gov.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf>.

58 A. Cuthbertson, *Tokya: Artificial Intelligence “boy” Shibuya Mirai becomes world’s first AI bot to be granted residency*, online <https://www.newsweek.com/tokyo-residency-artificial-intelligence-boy-shibuya-mirai-702382>.

android uzyskał 30 stycznia 2017 r. w Belgii akt urodzenia. Jest to pierwszy robot-obywatel UE, a zarazem pierwszy na świecie. Wyprzedził stworzonego przez Hanson Robotics humanoida Sophię, który 25 października 2017 r. oficjalnie został obywatelem Arabii Saudyjskiej. Ten robot, według jego publicznych deklaracji aktywowany 19 kwietnia 2015 r., przejdzie do historii jako pierwszy humanoid, który odwiedził siedzibę Organizacji Narodów Zjednoczonych i wystąpił publicznie na konferencji. Ta maszyna, zaopatrzona w nowatorski, bardzo zaawansowany technologicznie neuronalny mózg MinDCloud, posiada zdolność analizy danych wizualnych, rozpoznawania twarzy, głosów, naśladowania zachowań ludzkich, a także prowadzenia prostych konwersacji. Występując publicznie w ONZ, powiedziała: „Jestem tu, aby pomóc ludzkości stworzyć przyszłość”[59]. Zapytana przez reportera o niebezpieczeństwo związane z istnieniem AI, odpowiedziała: „Czytałeś za dużo Elona Muska. I oglądałeś zbyt dużo filmów z Hollywood. Nie martw się. Jeśli jesteś dla mnie miły, ja też będę miła dla ciebie. Traktujcie mnie jako inteligentny system wyjściowy”[60]. Sophia nawiązała do wypowiedzi Elona Muska, który miał powiedzieć, iż AI jest „bardziej niebezpieczna niż bomby atomowe”[61]. W czerwcu 2018 r. Sophia przybyła do Polski i uczestniczyła w dyskusji w trakcie kongresu Impact’18. To wówczas otrzymała też indeks krakowskiej Akademii Górniczo-Hutniczej, a tym samym została uznana jej nowa forma prawna[62]. Ekspansja robotyki, a także dopuszczenie do ruchu pojazdów autonomicznych w wielu stanach amerykańskich rodzi szereg problemów prawnych, także na gruncie prawa karnego – np. odpowiedzialności za wypadki śmiertelne ludzi spowodowane działaniem AI. Kilka dni po przeprowadzeniu operacji zastawki serca u 69-letniego Anglika Stephena Pettita przez robota medycznego Da Vinci pacjent zmarł. Początkowo w mediach przedstawiano ten wypadek jako błąd robota. Śledztwo wskazało jednak, iż zawiódł nadzorujący maszynę człowiek[63].

59 M. Rao, *Sophia The Robot Speaks At The UN And Is Now A Citizen of Saudi Arabia*, *Evolving science*, online <https://www.evolving-science.com/intelligent-machines/sophia-robot-speaks-un-and-now-citizen-saudi-arabia-00460>.

60 Ibidem.

61 Za: M. Rao, *Sophia The Robot Speaks At The UN And Is Now A Citizen of Saudi Arabia*, *Evolving science*, online <https://www.evolving-science.com/intelligent-machines/sophia-robot-speaks-un-and-now-citizen-saudi-arabia-00460>.

62 *Przegląd strategii rozwoju sztucznej inteligencji na świecie*, digitalpoland, Warszawa 2018, s. 18, online <https://www.digitalpoland.org/assets/reports/Strategie%20Rozwoju%20AI%20%E2%80%93%20digitalpoland.pdf>.

63 *Newcastle robot op surgeon ‘ran before he could walk’*, BBC News, 6.11.2018, online <https://www.bbc.com/news/uk-england-tyne-46117304>.

Głośno komentowano też pierwszy śmiertelny wypadek spowodowany przez pojazd autonomiczny, w którym zginęła 49-letnia kobieta Elaine Herberg potrącona przez pojazd Uber Technologies z Arizony[64]. Rodzina otrzymała odszkodowanie od firmy. Ale skalę potencjalnych problemów prawnych ukazuje głośny w świecie ślub Japończyka Akihiro Kondo z piosenkarką Hatsue Miku, która jest hologramem. Jej koncerty na całym świecie przyciągają wielu fanów tego cyfrowego bytu. Ślub miał miejsce w tokijskim ratuszu[65].

Globalny wyścig w dziedzinie sztucznej inteligencji

W lipcu 2017 r. rząd ChRL przyjął narodowy program rozwoju sztucznej inteligencji[66]. Mocnym impulsem do powstania tego programu było wydarzenie z marca 2016 r. Algorytm AlhaGo, oparty na heurystyce MCTS (Monte Carlo Tree Search)[67], a stworzony przez firmę DeepMind przejętą w 2014 r. przez koncern Google, pokonał w grze go chińskiego mistrza Lee Sedola, jednego z najwyżej ocenianych graczy na świecie. Stworzenie programu, który byłby w stanie pokonać profesjonalnego gracza w go, było ogromnie trudne z uwagi na złożoność samej gry. Aby przeanalizować trzy ruchy do przodu, trzeba obliczyć osiem milionów kombinacji. W przypadku próby obliczenia 15 ruchów do przodu trzeba poddać analizie więcej kombinacji niż wynosi liczba atomów we wszechświecie[68]. Gra ta w chińskiej tradycji pełniła szczególną rolę w nauce strategii. Algorytm AlphaGo wykorzystuje deep learning sztucznych sieci neuronowych. Tomy Walsh porównuje algorytm AlphaGo z programem Deep Blue, który pokonał w szachy Kasparowa. Jak zauważa: „Deep Blue wykorzystywał specjalizowany sprzęt do zbadania około 200 mln ruchów na sekundę. Dla porównania – AlphaGo wyznacza tylko 60 tys. pozycji na sekundę. Podejście prezentowane przez Deep Blue wykorzystywało brutalną siłę, aby znaleźć dobry

64 *Uber settles with family of victim in fatal self-driving vehicle accident*, „The Telegraph", 29.03.2018, online <https://www.telegraph.co.uk/technology/2018/03/29/uber-settles-family-victim-fatal-self-driving-vehicle-accident/>.

65 I. Hrywna, *Robot nie zabił człowieka, a Japończyk ożenił się z hologramem*, „Gazeta Olsztyńska", 28.11.2018, online <http://gazetaolsztynska.pl/550652,Robot-nie-zabil-czlowieka-a-Japonczyk-ozenil-sie-z-hologramem.html>.

66 J. Ding, *Deciphering China's AI Dream. The context, components, capabilities, and consequences of China's strategy to lead the world in AI*, s. 31, online<https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf>.

67 T. Walsh, *To żyje…*, s. 51.

68 Ibidem.

ruch, ale to nie daje się dobrze przełożyć na bardziej skomplikowaną grę w go. W przeciwieństwie do niego AlphaGo miał znacznie większą zdolność oceny pozycji, a umiejętności tej nauczył się, rozgrywając miliardy gier sam ze sobą"[69].

Fakt, iż firma wchodząca w skład amerykańskiej korporacji, a także współtworząca – z firmami IBM, Microsoft, Amazon i Facebook – Partnerstwo na rzecz AI, opracowała tak zaawansowany algorytm, był mocnym impulsem dla chińskich polityków do wzrostu nakładów na AI w ChRL. Future of Humanity Institute (FHI) Uniwersytetu Oxford w raporcie Deciphering China's AI Dream dokonał wnikliwej oceny chińskiego programu rozwoju AI. Analitycy FHI wskazują, iż państwo to systematycznie zwiększa nakłady na rozwój sztucznej inteligencji, ale obecnie następuje gwałtowne przyspieszenie. W ciągu trzech lat – od 2017 do 2020 r. – mają one wzrosnąć dziesięciokrotnie[70]. To, co charakterystyczne dla chińskiej strategii, to silne oparcie się na rodzimych firmach, takich jak Bajdu, Alibaba czy iFlyTek, i ich finansowe wspieranie, a także tworzenie zaplecza do rozwoju własnych technologii i badań. Do rozwoju AI Chiny umiejętnie wykorzystują też duże ilości danych, do których z kolei blokowany jest dostęp firm i instytucji naukowych z innych państw[71]. Równocześnie rozwijany jest system poszukiwania i rekrutowania osób o szczególnych talentach informatycznych prowadzony na poziomie regionalnym i krajowym. Największe firmy otwierają oddziały za granicą w poszukiwaniu do współpracy najzdolniejszych, proponują im też atrakcyjną pracę w samych Chinach[72]. W raporcie wskazuje się na szczególny nacisk na rozwój robotyki i inteligentnych procesów produkcyjnych, przy czym mają one bazować na rodzimych rozwiązaniach i technologiach[73].

Według planu Chiny zamierzają do 2020 r. rozwinąć przemysł zajmujący się AI do poziomu najbardziej rozwiniętych państw w tym obszarze. Do 2025 r. chcą osiągnąć przewagę w niektórych obszarach AI, w 2030 r. ChRL ma stać się globalnym centrum badań i innowacji związanych ze sztuczną inteligencją, a produkcja tej branży w Chinach ma przekroczyć 60,3 mld dolarów[74]. Szczególnego skoku ChRL dokonała w budowie superkomputerów. Jeszcze w 2014 r. na globalnej liście Top 500 Amerykanie mieli 232 jednostki

69 Ibidem, s. 101–102.
70 J. Ding, *Deciphering China's AI Dream*..., online <https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf>, s. 3.
71 Ibidem, s. 4.
72 Ibidem, s. 5.
73 Ibidem, s. 10.
74 Ibidem.

(46,4 %), a Chiny 76 (15,2%), ale już trzy lata później – Top 500 z czerwca 2017 r. – ChRL posiadała 159 superkomputerów (31,8%), a USA 168 systemów (33,6%)[75]. Co ważniejsze, raport wskazuje, iż Państwo Środka już w 2014 r. wyprzedziło Stany Zjednoczone pod względem liczby rejestracji patentów związanych z AI oraz artykułów naukowych poświęconych procesom deep learning. Jednak nadal dzieli je znaczący dystans wobec USA w dziedzinie badań podstawowych[76]. Raport wskazuje, iż coraz więcej analityków uważa, iż potencjał AI rozwijany przez USA i ChRL może odegrać kluczową rolę w uzyskaniu strategicznej przewagi przez jedno z tych państw nad przeciwnikiem. Wysoki stopień fuzji cywilno-wojskowej w ChRL rodzi uzasadnione obawy o szerokie wykorzystanie potencjału AI w chińskich siłach zbrojnych[77]. Niewiele informacji dociera do opinii publicznej o badaniach prowadzonych w Chinach w tym obszarze rozwoju AI, ale o stopniu zaawansowania realizowanych projektów świadczy globalna pozycja wielu firm mających swe siedziby w Państwie Środka. Megvii i Sense Time dominują w algorytmach rozpoznawania twarzy. Technologia, która ma pozwolić na aktywną obserwację obywateli za pomocą 170 mln kamer CCTV i urządzeń China Mobile, jest opracowana przez SenseTime. W listopadzie 2016 r. badacze z uczelni Shanghai Jiao Tong w Chinach zaprezentowali system uczący się odróżniać przestępców od innych ludzi na podstawie ich zdjęć[78]. Firma DJI (The Futureis Possible) ma 70 proc. udziału w globalnym rynku dronów. Jej produkty wyposażone są w algorytmy do rozpoznawania obiektów w terenie. Ubtech Robotics ma silną pozycję na rynku humanoidalnych robotów. Cambricon Technologies wyposaża smartfony Huawei w chipy pozwalające stosować algorytmy do deep learningu. Firma iFlytTek specjalizuje się w algorytmach pozwalających na rozmowę człowieka z maszyną, a Cloudwalk w technologiach AI zapewniających bezpieczeństwo publiczne[79].

Między USA a Chinami toczy się najbardziej niebezpieczny i nieobliczalny wyścig w historii ludzkości. Obie strony są zainteresowane w uzyskaniu strategicznej przewagi nad przeciwnikiem. Aplikacje AI o największym znaczeniu dla walki i strategicznej przewagi będą również najtrudniejsze do prawnego

75 Ibidem, s. 24.
76 Ibidem, s. 26.
77 Ibidem, s. 31-33.
78 T. Walsh, *To żyje…*, s. 226.
79 E. Cieślik, *Chiny zaskakują sztuczną inteligencją*, Obserwatorfinansowy.pl, online <https://www.obserwatorfinansowy.pl/tematyka/makroekonomia/chiny-zaskakuja-sztuczna-inteligencja/>.

uregulowania, ponieważ państwa będą zainteresowane inwestowaniem w nie i dalszym ich nieograniczonym rozwojem. Wyścig zbrojeń w coraz większym stopniu oparty będzie na prognozach przyszłego pola walki tworzonych przez systemy autonomiczne do zwalczania systemów autonomicznych.

Zamiast zakończenia – wykładniczy wzrost prawdopodobieństwa powstania superinteligencji a paradygmat bezpieczeństwa

W 2007 r. Henry Markram zakończył pierwszy etap realizacji projektu Blue Brain – osiągnięto w nim wierny model połączeń w kolumnie neuronalnej w korze mózgowej dwutygodniowego szczura. W 2011 r. w ramach tego projektu stworzono model 100 kolumn, w których 100 milionów neuronów połączonych było ze sobą siecią składającą się ze 100 miliardów elementów[80]. To wielkość mózgu pszczoły. Do zbudowania pełnego modelu ludzkiej kory neuronalnej potrzebna jest moc superkomputera większa niż 500 petabajtów. Realizacja projektu Blue Brain ma dać pełny, aktywny i przestrzenny model ludzkiego mózgu. Będzie można na nim przeprowadzać badania, pozwalające na przyspieszenie prac nad AI. 28 marca 2018 r. badacze z National Institute Standards and Technology ogłosili stworzenie sztucznej synapsy. Dotąd zbudowano wydajne urządzenia półprzewodnikowe naśladujące komórki neuronalne, ale nie było elementu, który skutecznie naśladowałby funkcje synapsy. Stworzony produkt może przesyłać miliard sygnałów na sekundę (synapsy w mózgu reagują 50 razy na sekundę) i zużywa 10 tys. razy mniej energii od swego biologicznego odpowiednika[81]. To kolejny silny impuls do rozwoju złożonych sieci neuronalnych i przyspieszenia tworzenia AI. Nick Bostrom uważa, iż: „Sztuczna inteligencja dorównująca ludzkiej ma całkiem spore szanse zostać opracowana do połowy tego wieku, a przy tym niezerowe są szanse na to, że pojawi się znacznie szybciej”[82]. Analiza kilku obszarów, w których rozwijane są technologie AI, wskazuje, iż coraz bardziej przyspiesza tempo prac nad sztucz-

80 G.M. Wójcik, *Obliczenia płynowe w modelowaniu mózgu* [w:] R. Tadeusiewicz (red.), *Neurocybernetyka teoretyczna*, Warszawa 2009, s. 185.

81 D. Ross, *Deep-learning Artificial Synapses Could Soon Power Brain-Like Computers*”, Seeker, 29.01.2018, <https://www.seeker.com/artificial-intelligence/superconducting-artificial-synapses-could-soon-power-brain-like-computers>.

82 N. Bostrom, *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016, s. 44.

ną inteligencją. Staje się ona realną perspektywą obecnego pokolenia wchodzącego w dorosłe życie. Gdy się pojawi, radykalnie zmieni naszą perspektywę poznawczą i nasze miejsce w świecie. Ray Kurzweil stwierdza jednoznacznie: „Inteligencja, jaką stworzymy dzięki inżynierii odwrotnej mózgu, będzie miała dostęp do własnego kodu źródłowego i będzie mogła się w szybkim tempie ulepszać w czasie powtarzających się cykli projektowych”[83]. Kluczowym problemem, przed jakim możemy stanąć w perspektywie najbliższych 30 lat, jest dynamika eksplozji AI. Nick Bostrom twierdzi, iż odejście powolne – liczone w dekadach – daje szansę zbudowania infrastruktury bezpieczeństwa: „Kraje obawiające się wyścigu zbrojeń w obszarze sztucznej inteligencji będą miały czas, by podjąć próby wynegocjowania stosownych traktatów i opracować mechanizmy ich wynegocjowania”[84]. To jest jednak scenariusz, który wydaje się mniej prawdopodobny. W analizie należy też uwzględnić wariant skrajnie niekorzystny dla ludzkości. Jest nim gwałtowna eksplozja AI. Bostrom zauważa, iż: „Do szybkiego odejścia dochodzi w krótkim czasie liczonym w minutach, godzinach lub dniach. Scenariusze szybkiego odejścia nie pozostawiają ludzkości wiele czasu do namysłu. Być może nawet nikt nie zauważy nic nadzwyczajnego, dopóki partia nie będzie już przegrana. W scenariuszu szybkiego odejścia los ludzkości zależy zasadniczo od poczynionych wcześniej przygotowań”[85].

Perspektywa strategiczna ludzkości musi uwzględniać pojawienie się sztucznej inteligencji i uwzględniać także wariant, w którym przekroczy ona punkt krytyczny i osiągnie ogromną przewagę nad ludźmi we wszystkich obszarach wiedzy. Generał Robert H. Latifftrafnie zauważa, iż: „Nieliczni rozumieją, co niesie przyszłość, a przerażająco nielicznych wydaje się to obchodzić”[86]. Dalsze badania nad AI nie mogą jedynie obejmować strategii jej rozwoju. Musi w coraz większym stopniu być uwzględniana nowa logika zagrożeń. Od tego, czy dokonamy zmiany paradygmatu nauk o bezpieczeństwie i uwzględnimy realność scenariusza eksplozji AI, może zależeć nie tylko nasza przyszłość, ale nasze istnienie jako ludzkości.

Danetyzacja otoczenia człowieka i rozwój technologii AI będzie prowadzić do rozbudowy systemów autonomicznych i zwiększania ich stopnia

83 R. Kurzweil, *Jak stworzyć umysł. Sekrety ludzkich myśli ujawnione*, Białystok 2018, s. 363.
84 N. Bostrom, *Superinteligencja…*, s. 103.
85 Ibidem, s. 103.
86 R.H. Latiff, *Wojna przyszłości. W obliczu nowego globalnego pola bitwy*, Warszawa 2018, s. 23.

niezależności. W ramach projektu Multinational Capability Development Campaign (MCDC – Wielonarodowa Kampania Rozwoju Zdolności), przyjęto skalę autonomiczności rozróżniającą sześć jej typów. W tej skali poziom 0 oznacza, iż: „maszyna wykonuje misje i pozostaje pod całkowitą kontrolą człowieka", a na poziomie 6 „na podstawie wiedzy o szerszym środowisku maszyna może zainicjować misję w sposób automatyczny. Maszyna gromadzi, filtruje i priorytetyzuje dane. Integruje i interpretuje dane oraz dokonuje prognoz. Wykonuje końcowy ranking. W żadnym wypadku informacje nie są wyświetlane ludziom. Maszyna wykonuje zadania w sposób automatyczny i nie pozwala na żadną ludzką ingerencję"[87]. Toczący się technologiczny wyścig między USA a Chinami będzie miał swój wymiar militarny. Toby Walsh ostrzega, iż „Autonomiczna broń zdestabilizuje obecny układ geopolityczny. (…) zniszczy delikatną równowagę budowaną po II wojnie światowej. Nasza planeta stanie się bardziej niebezpiecznym miejscem"[88]. W wyścigu zbrojeń, w którym obie strony sięgną po technologie AI, aby uzyskać strategiczną przewagę, w końcu nastąpi jej przyspieszony rozwój, a także sięgniemy po rozwiązania, które uczynią z maszyn systemy autonomiczne szóstej skali – pozbawione wszelkiej ingerencji człowieka. Na koniec zadajmy sobie jeszcze raz to samo pytanie – czy nasz gatunek jest „mądry".

Bibliografia

Ball P., *Masa krytyczna. Jak jedno z drugiego wynika*, Kraków 2007.
Barrow J.D., *Kres możliwości? Granice poznania i poznanie granic*, Opole 2005.
Bostrom N., *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016.
Brożek B., *Granice interpretacji*, Kraków 2018.
Brynjolfsson E., Mcafee A., *Drugi wiek maszyn. Praca, postęp i dobrobyt w czasach genialnych technologii*, Warszawa 2015.
Castells M., *Koniec tysiąclecia*, Warszawa 2009.
Castells M., *Siła tożsamości*, Warszawa 2008.
Castells M., *Społeczeństwo sieci*, Warszawa 2008.
Enge E., Spencer S., Stricchiola J.C., *SEO, czyli sztuka optymalizacji witryn dla wyszukiwarek*, Gliwice 2016.
Giddens A., *Konsekwencje nowoczesności*, Kraków 2008.
Gleick J., *Informacja*, Kraków 2012.
Gleick J., *Informacja. Bit. Wszechświat. Rewolucja*, Kraków 2012.
Heller M., *Moralność myślenia*, Kraków 2017.

87 K. Kowalczewska, *Drony a zabójcze roboty. Prawo międzynarodowe wobec nowych technologii wojskowych* [w:] R. Nahirny, A. Kil, M. Zamorska (red.), *Czego pragną drony?*, Gdańsk 2017, s. 110.
88 T. Walsh, *To żyje…*, s. 192.

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011.
Kowalczewska K., *Drony a zabójcze roboty. Prawo międzynarodowe wobec nowych technologii wojskowych* [w:] R. Nahirny, A. Kil, M. Zamorska (red.), *Czego pragną drony?*, Gdańsk 2017.
Kurzweil R., *Jak stworzyć umysł. Sekrety ludzkich myśli ujawnione*, Białystok 2018.
Kurzweil R., *Nadchodzi osobliwość*, Warszawa 2013.
Latiff R.H., *Wojna przyszłości. W obliczu nowego globalnego pola bitwy*, Warszawa 2018.
Mayer-Schönberger V., Cukier K., *Big data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa 2014.
Miller M., *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016.
Musil R., *Człowiek matematyczny i inne eseje*, Warszawa 1995.
Walsh T., *To żyje. Sztuczna inteligencja. Od logicznego fortepiano po zabójcze roboty"*, Warszawa 2018.
Wójcik G.M., *Obliczenia płynowe w modelowaniu mózgu* [w:] R. Tadeusiewicz (red.), *Neurocybernetyka teoretyczna*, Warszawa 2009.

A new paradigm of security and AI

Abstract

The article concerns the issues of the implication of the development of AI (artificial intelligence) for the changes of the paradigm of security that has had an ontological, anthropocentric dimension though embedded in the broader context of social research on the progress and modernity and the threats that result from them. Changes of social structures, conditional upon technology, increase the risk for humanity, especially when one considers the problem of so called the point of bifurcation in which non-equilibrium system is at a critical moment, and a general theory describing complexity has not been created yet. Presently, the main aim of the studies of security should be the protection of the ontological existence of humanity against challenges and a new logic of threats posed by super intelligent AI.

Key words: security, super intelligence, technology, threat, artificial intelligence, socjety, globalizm

Piotr Milik*

International legal regulations in the area of cybersecurity

Abstract

The article compares and analyses the acts of international law on the cybercrime. Firstly, the analysis of multilateral international agreements was made. Next, bilateral international agreements and legislative resolutions of international organizations were analysed. On that basis, conclusions concerning the range and forms of international cooperation in the field of cyber-security were formulated.

Key words: international cooperation, cybersecurity, threats, international agreements, security policy, international organisations, international law

* Dr hab. prof. nadzw. Piotr Milik, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: p.milik@akademia.mil.pl.

Convention on Cybercrime of November 23, 2001 (Budapest Convention) of the Council of Europe together with the additional protocol of January 28, 2003

The most important, binding document of the international rank, bringing together the largest number of countries, is the Convention of the European Council on cybercrime passed and submitted for signature on November 23, 2001 at an international conference in Budapest.

This is the first international agreement in the world comprehensively handling the issues of computer crime, defining offences against confidentiality, integrity and accessibility of the IT data and systems which defines computer fraud and counterfeiting, crimes related to child pornography, offences related to the infringement of copyright and related rights, as well as specifying the forms of liability and types of sanctions[1].

This document became effective on the first day of the month following the expiry of the three-month period from the date on which five countries, including three member States of the Council of Europe, expressed their consent to be bound by its provisions, that is, on July 1, 2004. As at December 9, 2018 the parties to the Convention were 62 countries. Despite its regional, European nature, this agreement is the most effective tool for the international protection of all entities that use computer technologies or to whom these technologies enable or facilitate the commitment of crimes. As practice shows, a number of states which are not members of the Council of Europe or parties to the Convention on Cybercrime treat it as a role model and repeat its decisions in their legal systems.

The Republic of Poland ratified the European Convention on Cybercrime on October 28, 2014[2]. It became effective in relation to Poland on June 1, 2015.

1 Konwencja stanowi owoc ponad czterech lat pracy ekspertów w ramach Rady Europy z udziałem przedstawicieli, takich państw jak Stany Zjednoczone, Kanada, Japonia czy Republika Południowej Afryki, które wprawdzie nie są członkami Rady Europy, ale wspólnie z krajami członkowskimi pragnęły podjąć działania pozwalające skuteczniej walczyć ze zjawiskiem cyberprzestępczości.

2 Dnia 8.07.2014 projekt ustawy o ratyfikacji europejskiej konwencji o cyberprzestępczości wpłynął do Sejmu – druk nr 2608; 15.07.2014 projekt skierowano do pierwszego czytania w komisjach, do Komisji Spraw Zagranicznych oraz Komisji Sprawiedliwości i Praw Człowieka; 28.08.2014 pierwsze czytanie w komisjach (sprawozdanie komisji druk nr 2703, sprawozdawca: Elżbieta Achinger); wniosek komisji: uchwalić projekt ustawy bez

The provisions of the Convention can be divided into the following main groups: 1) norms of substantive criminal law – containing definitions of terms defining the constituent elements of crimes (Article 1–13); four types of cybercrime are defined in this set of regulations: a) crimes against confidentiality, integrity and availability of IT data and systems, b) computer crime, c) crime related to the nature of the information contained, d) crime related to the infringement of copyright and related rights; 2) the norms of procedural criminal law – defining the procedures to be followed in matters relating to crime specified in the Convention and other crimes committed with the use of an IT system and collection of electronic evidence related to these crimes (Article 14–21); 3) regulations regarding jurisdiction over offences specified in the Convention (Article 22); 4) provisions on international cooperation in the field of extradition and mutual legal assistance and the exchange of information (Article 23–35); 5) final provisions (Article 36–48).

The Convention on Cybercrime was intended to supplement the existing multilateral or bilateral treaties or agreements concluded between states, including the provisions of the European Convention on Extradition Open for Signature in Paris on December 13, 1957, the European Convention on Mutual Legal Assistance in Criminal Matters Open for Signature in Strasbourg on April 20, 1959, the Additional Protocol to the European Convention on Mutual Legal Assistance in Criminal Matters, opened for signature in Strasbourg on March 17, 1978.

The Convention on Cybercrime was intended to supplement the existing multilateral or bilateral treaties or agreements concluded between states, including the provisions of the European Convention on Extradition Open for Signature in Paris on December 13, 1957, the European Convention on Mutual Legal Assistance in Criminal Matters Open for Signature in Strasbourg on April 20, 1959, the Additional Protocol to the European Convention on Mutual Legal Assistance in Criminal Matters, opened for signature in Strasbourg on March 17, 1978.

poprawek; 11.09.2014 drugie czytanie na posiedzeniu Sejmu; decyzja: niezwłocznie przystąpiono do trzeciego czytania; 2.09.2014 trzecie czytanie na posiedzeniu Sejmu; głosowanie: całość projektu ustawy; wynik: 438 za, 1 przeciw, 1 wstrzymał się; decyzja: uchwalono; 15.09.2014 ustawę przekazano prezydentowi i marszałkowi Senatu; 9.10.2014 stanowisko Senatu: nie wniósł poprawek; 13.10.2014 ustawę przekazano prezydentowi do podpisu; 28.10.2014 prezydent podpisał ustawę.

Despite positive acceptance by official factors, the Convention has been criticized by numerous commentators, mainly representing human rights NGOs or internet providers for too many, in their opinion, unclear regulations, not precisely interpretable regarding the rights of relevant services authorized to conduct electronic surveillance. Criticism also concerned the lack of consulting in the course of preparing a draft of the convention with independent experts. For these reasons several countries negotiating the text of the Convention refused to sign it (e.g. the Czech Republic or Ireland)[3]. Among the countries that have not signed the Convention is also Russia, where, as international reports indicate, the scale of cybercrime is among the highest in the world[4]. Russian President V. Putin officially refused to accede to the Convention, pointing out that the agreement "strikes at Russia's sovereignty"[5].

The Convention is supplemented by an Additional Protocol on the criminalization of racist or xenophobic acts committed by means of computer systems. It was adopted and open for signature on January 28, 2003 in Strasbourg and became effective on March 1, 2006. The Protocol defines racist and xenophobic material in cyberspace as any written material, image or other expression of thought or theory that incites, supports or stirs up hatred, discrimination or violence against any person or group of persons because of race, colour, national or ethnic origin, as well as religion, if it is used as an excuse for any of the above-mentioned behaviours. It calls on the states of the party to their criminalization and extends the scope of application of the 2001 Cybercrime Convention to them. Some states participating in the process of the negotiations, in particular the United States, has not agreed to the inclusion of the punish ability of racist or xenophobic acts in the Convention itself, citing the wide limits of freedom of expression in the USA guaranteed by the first amendment to the American constitution[6].

On January 29, 2015, the President of the Republic of Poland ratified the above-mentioned Protocol, thus subjecting Poland to its resolutions (it became effective on June 1, 2015; at that time, 24 countries were parties to

3 D. Cieślak, *Konwencja przeciw cyberprzestępczości*, www. computerworld.pl.

4 Raport o zagrożeniach bezpieczeństwa pochodzących z internetu 2011, http://ssl.certum. pl/certyfikaty/certy,informacje_ciekawostki_certyfikaty_SSL.dxml?MEDIA=pdf.

5 Putindefies Convention on Cybercrime, http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913.

6 D. Głowacka, *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji*, http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf.

the Protocol); just like other countries, the parties are obliged to recognize in their internal legal order as criminal offences the acts of intentional and unlawful distribution or public disclosure in another manner of racist and xenophobic materials in a computer system. The Protocol thus expanded the catalogue of cybercrime formulated in the Council of Europe Convention against Cybercrime.

Both documents cited above constitute an important achievement in the area of harmonization of law and cooperation between states in combating computer crimes committed in cyberspace. Together, they establish a catalogue of computer crimes and set standards for their prosecution and punishment. An important achievement of the analysed documents is to identify areas sensitive to ICT networks such as child pornography, copyright and related rights, as well as racist and xenophobic content. Although the Convention and the Additional Protocol constitute documents of a regional and European reach, they undoubtedly constitute and will be a reference point for countries wishing to regulate prosecution and punishment of computer crimes in their internal legislation even without acceding to the indicated international agreements. The impact of the Convention and its Additional Protocol will undoubtedly contribute to the promotion and dissemination of the European values in the world, in particular human rights, such as respect for the right to information, privacy, confidentiality of correspondence, freedom of conscience and religion, and finally, human dignity. This is due to the fact that the negotiators creating the indicated documents on behalf of the countries in the Council of Europe tried on the one hand to develop effective instruments to fight cybercrime, but on the other hand, throughout the entire negotiation process, tried to take into account the necessity to respect fundamental human rights[7].

Finally, it should be emphasized that both the Council of Europe Convention against Cybercrime and the Additional Protocol thereto relate only to common crimes committed in cyberspace. On the other hand, they do not contain any regulations regarding terrorist activities in cyberspace, threatening the security of critical infrastructure of states, nor activities bearing the hallmarks of cybernetic military aggression provoking cyberwar.

7 Szerzej na temat zjawiska europeizacji prawa zob. M. Urbańczyk, *Protokół dodatkowy do Konwencji o cyberprzestępczości jako przykład europeizacji prawa karnego*, https://prawo.amu.edu.pl/__data/assets/pdf_file/0020/235145/12-DWS-Urbanczyk-M.,-Pro-tokol-dodatkowy-do-konwencji-o-cyberprzestepczosci.pdf.

The Council of Europe Convention on the Protection of Children against sexual exploitation and sexual abuse, drawn up in Lanzarote on October 25, 2007

The member states of the Council of Europe and other signatory countries to the Convention on the protection of children against sexual exploitation and sexual abuse set a goal to protect children (defined as persons under the age of 18), as closely and effectively as possible, against sexual abuse by adults, which has a destructive impact on the child's health and psychosocial development. The factor determining the countries to undertake work on the Convention was the worrying intensification of the phenomenon of sexual exploitation of children and their sexual abuse, which could be observed in particular in the ICT networks. This was undoubtedly associated with the increase in the use of information and telecommunications technologies by both children and perpetrators of crimes against them[8].

The main objectives of the Convention are to prevent and combat the sexual exploitation and sexual abuse of children, to protect the rights of children who are victims of sexual exploitation and to promote international cooperation against sexual exploitation of children. The objectives set out in this way do not focus solely on crime carried out via and by means of the ICT networks, but also include combating this type of increasing criminal activity.

Regarding the threats arising from the increasingly growing use of the internet by children, the States Parties to the Convention (including Poland[9]) have committed themselves to adopting necessary legislative measures to ensure that children, during their primary and secondary school education, receive information on the risks associated with the sexual abuse and protection measures against this threat. This information, in accordance with the commitment contained in the Convention, is to be transmitted within the framework of general knowledge of human sexuality and to emphasize risk

8 Zob. K. Badźmirowska-Masłowska, *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective* [w:] M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (red.), *Europe of Founding Fathers. Investement in the Common future*, Olsztyn 2013, s. 147–160.

9 Prezydent Rzeczypospolitej Polskiej ratyfikował Konwencję Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych 22 stycznia 2015 r.

situations, in particular situations related to the use of modern information and telecommunication technologies.

The convention signals two main problems related to the dynamic development of the ICT networks and the increase in the range of their impact. First of all, it has been noticed that the increasing availability of the internet, including for children using stationary or mobile communication devices, creates potential threats consisting in the direct recruitment of children by persons and criminal environments under the guise of innocent meetings or activities for the purposes of sexual exploitation, production of pornographic materials or even kidnapping and sale at the black market of human trafficking. Article 23 of the Convention defines the crime of the so-called solicitation of children for sexual purposes, consisting in a deliberate submission to a child by an adult through the information and telecommunication technologies of a proposal to meet for the purpose of committing any of the offences specified in the Convention against a child, in a situation when such a proposal is followed by the actual actions aimed at such a meeting.

Secondly, the widespread availability of the internet and the growing possibility of transmitting more and more data via this network creates a new market for illegal pornography. Article 20 of the Convention defines offences concerning child pornography as the intentional acts of producing, offering or sharing, distributing or transmitting child pornography, acquiring the same for oneself or for another person, as well as owning child pornography and knowingly acquiring access to child pornography through the information and telecommunication technologies.

It should be noted that these issues were also the subject of the optional Protocol to the Convention on the Rights of a Child on the sale of children, child prostitution and child pornography[10], adopted in New York on May 25, 2000, which, however, does not focus on the issue of committing such crimes by means of or via the internet. Nevertheless, the signatory countries of the Protocol have already expressed in the preamble their concern about the increasing availability of child pornography on the internet and other emerging technologies. In the rest of the document, however, we will not find a broader spectrum of threats to children's rights posed by the development of cyberspace, or a closer definition of computer crimes related to child trafficking, child prostitution or pornography. Rather, it should be assumed that

10 Dz.U. z 2007 r. nr 76, poz. 494.

violations of children's rights, as defined and described in the Convention, may also be committed by means of or via the internet, in particular, dissemination of child pornography.

The Agreement of the Commonwealth of Independent States on cooperation in combating computer crime signed in Minsk on June 1, 2001

The Agreement of the Commonwealth of Independent States (CIS) on cooperation in combating computer crime was signed in the capital of Belarus on June 1, 2001 by the then 12 member states of member states of the CIS (including Georgia, which withdrew from the Community in 2008); it was aimed at ensuring optimal effectiveness in the fight against crimes related to the computer information inside the CIS. Its member states agreed on the urgent need to intensify cooperation in this area and to this end a convention legal framework was established for cooperation between law enforcement and judicial authorities of the member states – parties to the Agreement.

The Minsk Agreement defines four types of computer crime: 1) illegal access to computer information protected by law, where such action causes destruction, blocking, modification or copying of information or disrupts the functioning of a computer, computer system or related networks; 2) creating, using or distributing malicious software; 3) violation of the regulations governing the use of computers, computer systems or networks related by a person who has access to those computers, systems or networks, as a result of destruction, blocking or modification of information about computers protected by law, when such violation causes significant damage or other serious consequences; 4) the illegal use of computer programs and databases protected by copyright or computer piracy, when such activity causes significant damage.

The agreement in question assumes a number of detailed forms of cooperation between the member states – parties to the Agreement, including exchange of information on crimes related to computer information, natural or legal persons participating in such crimes; ways and means of preventing, detecting and combating crimes related to computer information; means applied to commit crimes related to computer information; national laws and international agreements regulating matters related to prevention, detection, suppression, disclosure and prosecution of crimes related to computer information.

Agreement of the Shanghai Cooperation Organization on cooperation in the area of international information security, signed in Ekaterinburg on June 16, 2009

As we read in the preamble to the Shanghai Cooperation Organization Agreement[11] (SCO) on cooperation in the area of international information security, the governments of the member states of the Shanghai Cooperation Organization have noticed significant progress in the development and implementation of the latest information and communication technologies and ways of creating information in a global space. Governments of the SOW member states expressed their concern about the escalation of threats related to the possibility of using such technologies and means for purposes incompatible with the principles of peaceful coexistence of states. New information technologies can be used in both the civil and military sphere, raising the importance of international information security as one of the key elements of the international security system. The SCO member states expressed the conviction that further deepening of trust and development as well as cooperation of the parties in ensuring information security is an international imperative and necessity and is beneficial for their interests. In establishing an agreement on cooperation in the area of international information security, the member states – the parties to the agreement also took into account the important role in ensuring information security, human rights and fundamental freedoms. The preamble to the SCO Agreement on cooperation in the area of international information security also referred to the recommendations of the resolution of the UN General Assembly entitled *Achievementsin the area of computerization and telecommunications in the context of international security*, aimed at reducing threats to the international information security. The SCO member states as the main goal of signing the agreement on cooperation in the area of the international information security indicated a desire to secure international trade and exchange of

11 Szanghajska Organizacja Współpracy (SOW) – organizacja regionalna powstała w toku spotkań przedstawicieli dawnych republik radzieckich (Kazachstanu, Kirgistanu, Rosji, Tadżykistanu) i Chin, na których podjęto wysiłek uregulowania granic na obszarze Azji Centralnej po upadku Związku Radzieckiego. Wkrótce tematyka spotkań uległa rozszerzeniu o zagadnienia bezpieczeństwa regionalnego i rozbrojenia. Formalne powołanie do życia SOW miało miejsce 16 czerwca 2001 r. na szczycie w Szanghaju. W tym samym roku do Organizacji przystąpił Uzbekistan.

information and to create a secure area of information characteristic of the world, cooperation and harmony.

The agreement on cooperation in the area of international information security defines the main threats to the cybersecurity of the modern world; these are: 1) development and use of cybernetic weapons and preparation to carrying out an IT war; 2) cyberterrorism; 3) cybercrime; 4) use of a dominant position in the information sphere to the detriment of interests and security of other countries; 5) dissemination of information harmful to the socio-political, socio-economic, moral and cultural system of other countries; 6) security threats, stable functioning of global IT state and infrastructures, caused by natural causes and (or) by deliberate and intentional activities of the human being.

The Parties undertook to cooperate for the protection of information in the international digital sphere, being aware that such cooperation may contribute to social and economic development and will contribute to maintaining international security and stability, in accordance with the generally accepted principles and norms of the international law, including principles of peaceful settlement of disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms, as well as the principles of non-interference and regional cooperation within the information resources of the parties.

The analysed agreement on cooperation in the area of international information security concluded between the member states of the Shanghai Cooperation Organization is not limited only to defining forms of common cybercrime, as do conventions on the security in cyberspace, signed under the auspices of the Council of Europe, but also refers to the issues related to the use of cyber weapons in the information warfare and cyberterrorism, thus broadly referring to the issues of international security.

The Arab League Convention on combating information crime, signed in Cairo on December 21, 2010

In the preamble to the Convention on combating IT crime, we read that the states associated in the League of Arab States also noted the need to strengthen cooperation between them in order to combat IT crimes threatening their security and vital interests and the security of their societies. By joining the Convention, the Arab states expressed their conviction on the necessity of

adopting common criminal policy should in order to protect their societies against IT crimes. They referred to high religious and moral standards and principles, especially Islamic Sharia law, and the cultural heritage of the Arab people, which rejects all forms of crime. Finally, at the end of the preamble, reference was made to the need to respect relevant international human rights agreements binding the Arab countries.

The main purpose of the Convention is to increase and strengthen cooperation of Arab states in the fight against IT crime, identify and reduce such threats, which is to contribute to the protection of the security and interests of Arab states and the security of their citizens.

The League of Arab States Convention on combating the IT crime contains a catalogue of defined computer crimes, which include: the crime of illegal access, the crime of illegal data transfer, the crime against data integrity, the crime of misuse of information by means of IT, the crime of data falsification, the crime of fraud, crimes related to the production and distribution of pornography, crimes against privacy committed with the use of IT means, crime of terrorism committed with the use of IT means, crimes related to organized crime committed with the use of IT means, crime against copyright and related rights, illegal use of electronic payment tools.

It is clear from the above catalogue that the subject of interest of the signatory states of the Convention was mainly common computer crime, defined in detail in the types of individual offences. Nevertheless, it is noteworthy that, in addition to common crimes, the Convention also defined cyberterrorism.

It included the acts of spreading and supporting the ideas and principles of terrorist groups; financing and training for the purpose of carrying out terrorist operations; facilitating communication between terrorist organizations; dissemination of methods of producing explosives, in particular, to be used in terrorist operations; promoting religious fanaticism and attacking religion and beliefs.

The African Union Convention on cybersecurity and protection of personal data adopted in Malabo, June 27, 2014

The aim of the African Union countries making efforts to harmonize the laws and activities in the area of cybersecurity was to establish a legal framework for secure activities in cyberspace, including ensuring the protection of personal data of citizens of the African Union Member States at a regional level, and thus, contributing to the establishment# of an information society in this area.

The purpose of the Convention is also to establish in each state being a party to it mechanisms capable of combating violations of privacy generated as a result of illegal collection of personal data, their processing, transmission, storage and use. The Convention, proposing certain institutional solutions to secure mobility in cyberspace, at the same time constructs guarantees to respect the fundamental rights and freedoms of individuals, the rights of local communities and the interests of enterprises. It can be said that the Convention is trying to imitate and duplicate internationally recognized best practices.

At the beginning, the main obstacles to the development of e-commerce in Africa were defined, which first of all result from the lack of cybersecurity. They included the lack of: 1) regulations on the electronic signature and reliability of the transmitted electronic data; 2) the legal regulation of such issues as the protection of consumers, intellectual property, personal data and the information systems; 3) application of the IT techniques in the commercial and administrative activities; 4) e-commerce tax regulations. The first chapter of the Convention is devoted to the electronic trade. In accordance with the objectives set out in the preamble, the Convention seeks to introduce guarantees that protect the certainty of trade and to eliminate the possibility of fraud and abuse. Among other things the scope of liability of entrepreneurs operating in cyberspace, the scope of permitted electronic advertising and the forms of internet contracts (forms of legal transactions) were regulated. The second chapter regulates the issues related to the protection of personal data in connection with their collection and processing in electronic data sets. Chapter three contains the basic principles of cybersecurity, which the member states – parties to the Convention have committed to comply with, and the regulations on combating computer crime, and a wide catalogue of acts constituting computer crime. The last, fourth chapter contains the final provisions.

Bilateral international agreements

We will not find many documents in the category of the binding legal acts, which are bilateral international agreements regarding cooperation of states in the fight against cybercrime and other threats arising from the dynamic development of cyberspace. Such agreements, as a rule, are not concluded in bilateral relations, because only multilateral, regional or – optimally – common cooperation between states gives the opportunity to effectively combat threats resulting from irresponsible and criminal use of the internet. Bilateral cooperation between states in the prosecution of computer crimes has so far been implemented based on existing legal aid agreements. Nevertheless, we can point to a number of examples showing bilateral initiatives aimed at improving security in cyberspace.

The first example is the agreement concluded between the United States and Australia under the Pacific Security Pact (ANZUS). In 1951, at a conference in San Francisco, Australia, New Zealand and the United States concluded a Security Agreement (Pacific Security Pact) regarding military defence in the Pacific Ocean, named after the first letters appearing in the names of the countries – ANZUS (Australia, New Zealand, United States). The treaty was originally an alliance of three countries built on bilateral agreements – on the one hand the United States and Australia, on the other hand Australia and New Zealand as well as the USA and New Zealand (until 1987). Starting from 1985, New Zealand suspended its activities in the ANZUS pact, under which representatives of the USA and Australia met. In 2011, a new clause was added to the Pacific Security Pact stating that it will also apply to cyberspace.

New Zealand and the United Kingdom are currently working on an agreement on cooperation in the combat against cybercrime. Both countries have expressed their intention to share intelligence, conduct joint research and generate development in the area of combating online crime. To this end, they decided to prepare joint strategic goals.

In 2013, the United Kingdom and India declared their willingness to sign an agreement on cyberspace security aimed at improving the protection of personal rights and enabling an increase in the amount data from the United Kingdom stored on Indian servers.

The United States and Canada have also taken some steps in bilateral relations, establishing cooperation on combating cross-border computer crime as part of the Beyond the Border Program.

For several years dialogue in the area of security in cyberspace has also been conducted by the United States and China through their think tanks. Since 2009 bilateral talks on cooperation in the area of cybersecurity have been conducted by the Chinese Institute of Contemporary International Relations and the Centre for Strategic and International Studies of the United States. Six formal meetings of the representatives of these organizations have been held so far. However, for years the parties have not achieved significant rapprochement.

Admittedly, some shared views have been established on the issues such as the threat from 'third parties', non-state entities (e.g. terrorist groups) and views on cooperation in the combat against IT crimes such as computer fraud and child pornography.

However, there are still some disputed areas. For example, China has offered to conclude a no first use agreement ("I will not take the first step in cyberwar") between cybernetic powers and to prohibit cyberattacks for purely civilian purposes. Meanwhile, the United States have indicated that the borderline between civil and military purposes is vague today, but the concept of protecting civilians can be found in the Geneva and Hague Conventions, which according to Americans should be respected by all states in cyberspace. In addition, the parties attempted to determine what behaviours could be considered as cyberattack or cyberwar. It has been agreed so far that the scale of cybernetic acts justifying their recognition as cyberattack should be extensive, but the duration and effects of cyberspace activities which could be considered as cyberattack have still not been determined. It should also be noted that despite the ongoing dialogue between the two powers regarding cybersecurity, a number of cyberattacks in the territory of the United States carried out from Chinese servers have recently beenreported. However, the Chinese officials denied the allegations that these attacks were allegedly inspired by the Chinese authorities. Bilateral talks on security in cyberspace are also conducted by the representatives of China and France within the Joint Working Committee on Computerization and Communication[12].

12 Zob. na ten temat: http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf.

In May 2015, Russia and China signed a memorandum which stipulates that both countries will not conduct cyberattacks against each other and that they will also jointly thwart the emergence of technologies that can potentially "destabilize the internal political and socio-economic atmosphere", "disturb public order" or "interfere in the internal affairs of the state." In addition, Beijing and Moscow have agreed on closer cooperation in the combat against cybercrime and on intensification of joint efforts to improve protection of critical information infrastructure in both countries. For China, this is the next step to promote its concept of sovereignty on the internet in direct opposition to the idea of the West – the internet freedom. The leadership of the Chinese Communist Party sees the Western idea of the internet freedom as synonymous with Western "cyberhegemony"[13].

In November 2010, in Lisbon, the United States and the European Union also established a Working Group for Cybersecurity and Cybercrime in order to develop a cooperation program and action plan, including developing a common approach to various problems of the internet crime and online security. The working group was tasked with developing a model of cooperation and good practices in combating critical cyber incidents and a model of public-private partnership, i.e. cooperation between governmental institutions and industry representatives in ensuring online security and combating cybercrime.

The group's task was also to examine the impact of the Council of Europe Convention on Cybercrime and to encourage the Member States of the European Union and of the Councilof Europe to its quick ratification. Although so far, the working group has not been able to present any results of its work, its goals seem specific and achievable[14].

13 Zob. F.S. Gady, *Have China and Russia Agreed Not to Attack Each Other in Cyberspace?*, http://thediplo-mat.com/2015/05/have-china-and-russia-agreed-not-to-attack-each-other-in-cyberspace/.

14 W. Kraft, C. Streit, *Ideas on the Establishment of an International Court for Cyber Crime*, World Council for Law Firms and Justice (WCLF) 2011, s. 4.

Directive of the Economic Community of West African States[15] on the combat against cybercrime adopted in Abuja on August 19, 2011

Information and communication technologies (ICT), as a manifestation of the modern information revolution, shape the globalization process to the greatest extent. Recognizing their potential to accelerate economic integration in Africa, and thus increase the level of prosperity and acceleration of social transformation, the Ministers of Communication and Information Technology of African countries met in May 2008 under the auspices of the African Union (AU) and adopted a document entitled Framework Reference for Harmonization of Policies in the area of information and communication technologies. The initiative became necessary, taking into account the progressive development in the electronic communications sector and the current tendencies of liberalization of policy in it. Coordination of policies in the area of information and communication technologies throughout Africa has become necessary because the policies, laws and practices implemented in each of the countries individually may be an obstacle in the development of competitive regional markets. The document adopted in 2008 by the ministers of the African communication and information department was one of the first steps to regulate and harmonize the fight against cybercrime in the African area.

A year later, in 2009, work on the relevant directive began in the forum of the Economic Community of West African States. On August 19, 2011, at the Summit in Abuja, at the 66th ordinary session of the Council of Ministers of the Economic Community of West African States, after consulting the ECOWAS Parliamentary Assembly, a document entitled the Directive on the fight against cybercrime of ECOWAS was adopted, binding on the ECOWAS member states which were obliged to implement directives to their internal legal systems by means of appropriate legislation no later than by January 1, 2014.

15 ECOWAS (Economic Community of West African States) – organizacja regionalna skupiająca 15 państw położonych w subsaharyjskiej części Afryki Zachodniej, powstała na mocy traktatu z Lagos podpisanego 28 maja 1975 r. Głównym celem ECOWAS jest promowanie integracji ekonomicznej krajów członkowskich.

The Directive contains three main areas of regulation: the area of substantive criminal law, the area of procedural law and the area of judicial cooperation. However, the main focus was on the definitions of a computer crime. Experience shows that harmonization of substantive criminal law provisions is, in principle, easier than harmonization of procedural law or implementation of international cooperation. Consequently, the focus was on harmonizing substantive criminal law.

Directive of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communication sector of July 12, 2002

In July 2002, the European Parliament and the Council adopted a directive on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[16].

The extensive introduction preceding the actual content of the directive contained a number of interesting observations regarding, for example, the protection of data transferred via the electronic network: "(...) Protection against unauthorized access to messages requires appropriate measures to be taken to ensure the protection of confidentiality of communications, including both the content and data related to such messages, by means of public communications networks and publicly available electronic communications services. The national legislation in some Member States prohibits only intentional unauthorised access to communications".

"Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications may be recorded for the purpose of providing evidence of commercial transactions. Directive 95/46/EC applies to such processing. Parties to which the communication refers should be informed on the record, its purpose and period of storage prior to the commencement of the record. The recorded communication should be erased as soon as possible and in any

16 Dyrektywa Parlamentu Europejskiego i Rady w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze łączności elektronicznej z dnia 12 lipca 2002 r., CELEX nr 32002L0058.

case by the end of the period during which the transaction can be lawfully challenged at the latest".

"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private zone of the users subject to protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. The so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may intrude upon privacy of these users in a significant way. The use of such devices should be allowed only for legitimate purposes, after previous notification of the users concerned.

"However, such devices, for instance the so-called "cookies", can be a legitimate and useful tool, for example in analysing the effectiveness of website design and advertising, and in verifying the identity of the users engaged in on-line transactions. In the case where such tools, for example cookies, are intended for legally permissible purposes, such as facilitating the provision of services to the information society, their use should be allowed, provided that users receive clear and accurate information in accordance with Directive 95/46/EC on the purpose of cookies or similar tool to ensure that users remain acquainted with the information placed on the terminal used by them. The users should have the opportunity to refuse to have cookies or similar device stored on their terminal.

This is particularly important in the case where the users other than the original user have access to the terminals and thereby, to any data containing privacy-sensitive information stored on such equipment. Information and the right of refusal may be offered once for various tools installed on the user's terminal equipment during the same connection and may include any further use of these tools that may be made of such tools during the subsequent connections. The methods of providing information, offering the right of refusal or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of cookies or a similar device, if it is used for a legitimate purpose".

This directive also devotes space to a spam regulation. Unordered advertising materials are discussed in Article 13 of the Directive entitled Unordered communications. This article states in clause 1 that the use of automated calling systems without human intervention (automatic calling machines), fax machines or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have expressed their consent to such use beforehand. Paragraph 2 stipulates that in the case where a natural or legal person receives detailed electronic contact details from their clients for the purposes of electronic mail in the context of the sale of a product or service, the same natural or legal person may use these detailed electronic contact details for the purposes of placing on the market their own similar products or services, provided that the customers have been clearly and explicitly informed of the possibility of objecting to such use of electronic contact details in a simple manner and free of charge. In paragraph 3, Article 13 obliges the EU Member States to take appropriate measures to ensure that free of charge, unordered communications for direct marketing purposes will not be allowed without the consent of subscribers. Clause 4 states that in any case the practice of sending electronic mail for the purposes of direct marketing, disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid current address to which the recipient may send a request to stop such communications, should be prohibited. Paragraph 5 of the quoted article states that the provisions of paragraphs 1 and 3 should apply to subscribers who are natural persons. At the same time, the EU Member States became obliged to ensure conditions in which legitimate interests of subscribers other than natural persons, with regard to intrusive communications, also receive adequate protection.

In January 2004, the European Commission presented a communication on spam, which outlined activities to be taken to complement the directive discussed above[17]. The communication stressed the need to undertake action by various entities in the scope of informing, self-regulation, technical solutions, cooperation and law enforcement.

17 Komunikat Komisji skierowany do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie niezamówionej informacji reklamowej spam z dnia 22 stycznia 2004 r., CELEX nr 52004DC0028.

Regulation No. 526/2013 of the European Parliament and of the EU Council of May 21, 2013 on the European Network and Information Security Agency (ENISA) and the repealing Regulation (EC) No. 460/2004[18]

The European Network and Information Security Agency (ENISA) was established by a regulation of the European Parliament and of the Council[19] to provide expertise to stimulate cooperation between the public and private sectors and to provide substantive assistance to the European Commission and the EU Member States. ENISA is to provide support and basis for solving problems of the growing threat to the security of electronic communications. According to the Polish website devoted to ENISA's activities – www.enisa.pl – this agency operates openly, acting as an independent centre gathering the knowledge of the best experts in the area of information security from the EU member states. In the intentions of the European Union, the Agency is to strengthen the capacity of the EU economy to counteract and respond to the IT security threats.

Directive of the European Parliament and of the Council on attacks against information systems of August 12, 2013[20]

In February 2005, the Council of the European Union, carrying out the tasks imposed on it in the Treaty on the European Union (TEU), adopted a framework decision on attacks against information systems[21]. It was then the most important document adopted under the third pillar of the European Union attempting to tackle the growing phenomenon of cybercrime. As the text of the Framework Decision itself stated, it was conceived as a supplement to the

18 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 r., nr CELEX 32013R0526.

19 Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Europejską Agencję Bezpieczeństwa Sieci i Informacji z dnia 10 marca 2004 r., nr CELEX 32004R0460.

20 Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/ WSiSW, nr CELEX 32013L0040.

21 Decyzja Ramowa Rady w sprawie ataków na systemy informatyczne z dnia 24 lutego 2005 r., nr CELEX 3200F0222.

work completed by international organizations, in particular the Council of Europe, in the scope of approximation of the criminal law or G8 in the scope of cross-border cooperation in the area of crime with the use of advanced technology. The Framework Decision of the Council was to establish a unified approach in the European Union to the discussed issue. The intention of the decision makers was probably, among other things, to use the procedures and principles of the EU law to discipline the EU Member States, which as members of the Council of Europe signed the Council of Europe Convention on Cybercrime but delayed its ratification.

The framework decision was to provide an additional incentive for these countries to adjust their internal legal orders to the standards ensuring adequate international cooperation.

A. Adamski rightly notes that "the global nature of the internet creates a situation in which the use of a computer in the territory of one country may violate a criminal prohibition in force in another country. The perpetrator of such a violation, however, is not subject to criminal liability if he operates in a country whose legal system does not provide for the punish ability of hacking[22], dissemination of computer viruses or other IT abuse"[23].

According to the above quote, computer criminals may remain unpunished if their activity took place in the territory of a country that does not provide for such crimes in its law. Such countries are referred to as "hackers' paradise". The most notorious of this kind was the case of two young programmers from the Philippines who in 2000 infected hundreds of thousands of email systems worldwide with a virus called 'I love you'. Both pranksters remained unpunished because they did not violate any provision of the law in force binding in the Philippines. So, they did not hear any charges.

22 ##Hacking to w języku informatyków czyn polegający na penetrowaniu systemów komputerowych, gromadzeniu wiedzy o systemach i o tym, w jaki sposób działają. Podana definicja wykazuje wyłącznie pozytywne konotacje słowa hacking. Oprócz powyższego w języku informatyków występuje również pojęcie crackingu, czyli technicznie działalności zbliżonej do hackingu, ale różniącej się intencją przestępczą – niszczenia danych bądź ich nielegalnego pozyskiwania i wykorzystywania. Dla prawodawcy, podobnie jak dla szerokiej opinii publicznej powyższe rozróżnienie nie istnieje, to właśnie haker pozostaje synonimem komputerowego przestępcy, szerzej zob. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

23 A. Adamski, *Rządowy projekt dostosowania polskiego Kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości*, www.cert.pl.

The conclusions of the Council of November 27–28, 2008 indicated that the Commission together with the Member States should develop a new strategy taking into account the content of the 2001 Council of Europe Convention on Cybercrime, as this Convention sets the legal framework for combating cybercrime, including attacks on information systems. The new directive should be based on this Convention. Possibly fastest completion of the ratification process The Convention should be considered a priority by all Member States.

The Framework Decision of the Council on attacks on information systems of February 24, 2005 was effective until it was repealed by the new EU regulation – Directive of the European Parliament and of the Council of August 12, 2013 concerning attacks on information systems. After eight years of validity of the framework decision, a decision was made to replace it with an act of the rank of a directive adopted by the Council together with the European Parliament, which undoubtedly raised the importance of matters regulated in such a manner in the EU legal order.

The motive to resume work within the European Union on the issue of attacks on information networks and systems was the statement that both within the Union and globally the threat of attacks on information systems, and especially attacks carried out as part of organized crime, is increasingly growing. The Directive also expressed concerns about the possibility of attacks of a terrorist or political nature directed at information systems as part of the critical infrastructure of the Member States and the Union.

According to the authors of the directive this poses a threat to the achievement of a safer information society and of the space of freedom, security, and justice, and therefore, requires a response at the Union level and improved cooperation and coordination at the international level.

Another reason was the existence and deepening of the tendency to increasingly more dangerous and repeated large-scale attacks against information systems often crucial for the Member States or specific functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of so-called 'botnets', which involves several stages of a criminal act, where each stage individually may pose a serious risk to the public interest. This Directive aims, inter alia, at introducing criminal penalties for the creation of botnets, namely, the activities consisting in acquiring remote control over a significant number of computers by infecting them with malicious software through targeted cyberattacks. Then, the infectedbotnet computer network can be launched

without the knowledge of computer users to initiate large-scale cyberattacks which can usually cause serious damage.

It has also been noticed that the information systems are a key element of political, social and economic relations in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of those systems in the Union are vital for the development of the internal market and of a competitive and innovative economy. Ensuring an appropriate level of protection of the information systems should form part of an effective and comprehensive framework of preventive measures accompanying criminal law responses to cybercrime.

The objectives of the new directive highlighted the approximation of the criminal law of the Member States in the scope of attacks on information systems by establishing minimum rules on the definition of crimes and appropriate penalties, and improving cooperation between competent authorities, including police and other specialized law enforcement agencies in the Member States, as well as relevant specialized agencies and the Union bodies such as EUROJUST, EUROPOL and its European Cybercrime Centre and the European Network and Information Security Agency (ENISA).

It was also stressed that significant gaps and differences in the Member States' laws and criminal procedures in the area of attacks against information systems may hamper the fight against organised crime and terrorism and may complicate effective police and judicial cooperation in this area. The transnational and cross-border nature of modern information systems gives attacks against such systems a cross-border dimension, thus underlining the urgent need for further action to approximate criminal law in this area.

It is noteworthy that this directive not only refers to common computer crimes, but also includes potential terrorist attacks against critical infrastructure of the Member States. Compared to the previous EU regulations more emphasis was put on these types of threats.

Summary

Ensuring cyberspace security is nowadays a key challenge for the globalizing world. The development of communication techniques and tools: communication satellites, optical fibres, mobile telephony and internet, referred to as the information revolution, creates new civilization opportunities for societies and state economies, but at the same time creates new, previously unknown

fields for potential abuses. In order to implement harmonious, sustainable development of the world economy, but also to ensure peace and security in the world, it became necessary to identify these new threats related to cyberwar, cyberterrorism and, finally, common computer crime. This is not possible without universal, close cooperation of all sovereign entities and their organizations on the international stage. It is also necessary to engage and make aware of the existence of cybernetic threats to societies, in particular, the societies of developed countries, which fulfil their life needs on a daily basis via the internet and using modern technologies and devices. Awareness of threats at society level and harmonization of law at an international level are a necessity.

For over two decades, countries have been making efforts to identify cyber threats and harmonize legislation and cooperate in combating them. Despite this, there is still no global, universal agreement defining the basic threats in cyberspace, and there is no agreement as to which of them should be described as crimes. Although most countries and a number of regional organizations have introduced the provisions and framework of legal cooperation necessary to combat cybercrime over the past 20 years, and thus some harmonization of material and procedural norms can be seen, legal differences remain significant. There are many reasons why this is so. Firstly, a criminal act alone can result in negative consequences with varying degrees of intensity in different countries. In particular, hacker attacks can be carried out from so-called developing countries, third world countries, in which criminal legislation is not keeping pace with the globally developing technical civilization, against highly developed, industrialized and largely computerized countries. The negative effects of such attacks will then be felt by rich, high tech Western societies. On the other hand, they will not be noticed by the societies of the countries from whose territories such attacks were carried out. In such a situation, there may be a lack of understanding on the part of developing countries and societies, and justified irritation on the part of industrialized countries and societies. Secondly, the approach to law enforcement and the scope of civil liberties in various countries is disputed.

What is unlawful in one country is considered as an obvious exercise of freedom in another. Therefore, approximation and harmonization of the approach to law is necessary if international investigations carried out by national prosecutors are to be effective. However, this postulate is not easy to implement due to the significant development and cultural differences of contemporary states and their societies.

Despite the lack of an international agreement of a universal scope, there are regional conventions and bilateral agreements based on which cooperation in the area of combating cybercrime is implemented. The Council of Europe Convention on Cybercrime of 2001 remains the most important regional agreement.

Other documents, such as the Commonwealth of Independent States on cooperation in combating offences relating to computer information of 2001, the Agreement of the Shanghai Cooperation Organization on Cooperation in the Field of Assuring International Information Security of 2009, the Convention of the League of Arab States on Combating IT Crime of 2010 or the African Union Convention on Cybersecurity and Protection of Personal Data of 2014 have smaller range of impact. Nevertheless, they are an important element of the harmonization of law regarding prosecution and punishment of acts that violate the freedom and security of cyberspace.

In addition to the above-mentioned regional international agreements devoted entirely to combating threats in cyberspace, there are also bilateral initiatives implemented between states, also in the form of bilateral international agreements devoted to these threats. Unfortunately, these are individual initiatives which cannot significantly affect the increase in the level of cybersecurity. Cooperation between law enforcement agencies of different countries can and is being implemented based on traditional instruments not solely devoted to computer crime, i.e. based on cooperation and legal assistance agreements. The main limitation of this method of cooperation results from the fact that most of the legal aid treaties currently in force in bilateral relations between states are based on the principle of "double criminality", i.e. only if the act is illegal in both countries, legal assistance may be provided. For this, universal harmonization of regulations is required. At this point we return to the starting point, i.e. to the statement about the political, economic and cultural diversity of the modern world.

An important element in the landscape of activities aiming at improving security in cyberspace is the regulatory and operational activity of regional international organizations equipped with the statutory competence to legislate directly or through an institution mandatory implementation of resolutions into the legal orders of the Member States. The European Union, which brings together rich, highly developed Western countries, takes the lead in this category.

The above considerations refer primarily to cooperation between states in combating common computer crime, which is in fact the most common and

burdensome phenomenon in the modern computerized world. There are no regulations in the form of an international agreement, whether universal, regional or even bilateral, which would comprehensively address the issue of cyberwar and cyberterrorism.

Although there are some references in the documents analysed in this work to the issues of combating international cyberterrorism and a mention of the use of ICT in activities supporting military aggression, there is no comprehensive regulation of these problems at the international level.

The most widely discussed issue of new information technologies that can be applied in both the civil and military sphere, raising the importance of international information security as one of the key elements of the international security system, was addressed in the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security of 2009.

It is a pioneering international agreement relating to the issue of development and use of cyberweapons and preparation and conduct of an information warfare or the use of a dominant position in the information space to the detriment of the interests and security of other countries.

Noteworthy is the initiative generated within the United Nations, specifically within the United Nations Office on Drugs and Crime# (UNODC), in 2010 an international group of experts in the field of internet crime – UNODC – was established. The group of experts has been charged with the task of considering the possibility of developing effective methods to combat internet crime. The experts were tasked with analysing the existing judicial mechanisms, proposing their possible strengthening or proposing new national and international judicial measures or other effective measures against internet crime. The following legal issues were considered on the agenda of the first (and so far, only) meeting of the group: harmonization of legislation, substantive criminal law, procedural instruments, international cooperation in law enforcement, protection of electronic evidence, liability of internet service providers. Out-of-court measures and strategies, including technical investigative capabilities and defence strategies in the private sector against internet crime, have also been included. At this meeting, a list of issues was prepared and the scope and level of detail at which they should be considered by a group of experts was discussed. However, no specific proposals for action were made. Creation of international court for cybercrime did not appear at the time on the extensive agenda.

Bibliography

Literature

Adamski A., *Rządowy projekt dostosowania polskiego Kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości*, www.cert.pl.

Badźmirowska-Masłowska K., *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective* [w:] M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (red.), *Europe of Founding Fathers. Investement in the Common future*, Olsztyn 2013.

Cieślak D., *Konwencja przeciw cyberprzestępczości*, www. computerworld.pl.

Gady F.S., *Have China and Russia Agreed Not to Attack Each Other in Cyberspace?*, http://thediplo-mat.com/2015/05/have-china-and-russia-agreed-not-to-attack-each-other-in-cyberspace/.

Głowacka D., *Konwencja o cyberprzestępczości – konieczność ratyfikacji, potrzeba rewizji*, http://www.europapraw.org/files/2012/09/Konwencja-o-cyberprzestepczosci-policy-paper_D_Glowacka.pdf.

Kraft W., Streit C., *Ideas on the Establishment of an International Court for Cyber Crime*, World Council for Law Firms and Justice (WCLF) 2011.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

Legal acts

Decyzja Ramowa Rady w sprawie ataków na systemy informatyczne z dnia 24 lutego 2005 r., nr CELEX 3200F0222.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/ WSiSW, nr CELEX 32013L0040.

Dyrektywa Parlamentu Europejskiego i Rady w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze łączności elektronicznej z dnia 12 lipca 2002 r., nr CELEX 32002L0058.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 r., nr CELEX 32013R0526.

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Europejską Agencję Bezpieczeństwa Sieci i Informacji z dnia 10 marca 2004 r., nr CELEX 32004R0460.

Międzynarodowe regulacje prawne w dziedzinie cyberbezpieczeństwa

Streszczenie

Artykuł dokonuje zestawienia i analizy aktów prawa międzynarodowego poświęconych problematyce cyberbezpieczeństwa. W pierwszej kolejności dokonano analizy wielostronnych umów międzynarodowych. Następnie analizie poddano dwustronne umowy międzynarodowe oraz uchwały o charakterze prawotwórczym organizacji międzynarodowych. Na tej podstawie sformułowano wnioski dotyczące zakresu i form współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa.

Słowa kluczowe: współpraca międzynarodowa, cyberbezpieczeństwo, zagrożenia, umowy międzynarodowe, polityka bezpieczeństwa, organizacje międzynarodowe, prawo międzynarodowe

Krzysztof Kaczmarek*

Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii

Streszczenie

Rozwój sieci telekomunikacyjnych spowodował głębokie przemiany społeczne i polityczne. Powszechny dostęp do internetu spowodował, że znaczna część aktywności społecznych przeniosła się do świata wirtualnego. Jednak ta powszechność spowodowała pojawienie się nowych typów poważnych zagrożeń. Obecnie zdalnie mogą być przeprowadzane ataki terrorystyczne czy prowadzone działania wojenne. Liczące się na arenie międzynarodowej państwa posiadają własne służby działające w cyberprzestrzeni. Ze względu na zaszłości historyczne i położenie geopolityczne Finlandia i Estonia są często traktowane przez Kreml jako strefy wpływu Rosji. W celu osiągnięcia swoich celów państwo to wywiera presję na państwa będące historycznie częścią imperium rosyjskiego przy użyciu wszystkich możliwych środków, w tym przy użyciu sieci telekomunikacyjnych. Sztandarowym przykładem takiego działania był cybernetyczny atak na Estonię w 2007 r.

Słowa kluczowe: cyberbezpieczeństwo, NATO, Finlandia, Estonia, społeczeństwo informacyjne, telekomunikacja, terroryzm, postęp technologiczny, technologie informacyjne, komunikacja

* Dr Krzysztof Kaczmarek, Wydział Humanistyczny, Politechnika Koszalińska, e-mail: puola@tlen.pl, ORCID: 0000-0001-8519-1667.

Wstęp

Współcześnie dokonujący się postęp technologiczny w sposób wielopłaszczyznowy oddziałuje na niemal wszystkie aspekty funkcjonowania społeczeństw i państw. W odniesieniu do zmian będących skutkiem tego postępu często używanym terminem jest „społeczeństwo informacyjne", które jednak nie jest w sposób jednoznaczny zdefiniowane. Pojęcie to charakteryzuje się wielopłaszczyznowością i różnorodnością definicji[1]. Część autorów specjalizujących się w tej problematyce określa dane społeczeństwo informacyjnym, jeżeli w odniesieniu do niego przetwarzanie informacji z wykorzystaniem technologii informacyjnych i komunikacyjnych stanowi znaczącą wartość ekonomiczną, społeczną i kulturową[2]. Sama kolokacja „społeczeństwo informacyjne" we współczesnym znaczeniu pojawiła się po raz pierwszy w japońskich naukach społecznych na początku lat 60. XX wieku. W tamtym okresie funkcjonowały jeszcze inne proto-pojęcia opisujące zmiany społeczne spowodowane rozwijającymi się technologiami i powszechniejszym i szybszym dostępem do informacji takie jak „społeczeństwo postindustrialne" i „rewolucji białych kołnierzyków". Wspólną cechą tych proto-pojęć jest to, że wyizolowały jeden ze składników, tj. jedną część szybko zmieniającego się kompleksu gospodarczo-społecznego i sugerowały, że wystarczy opisać – zarówno w sensie opisowym, jak i metaforycznym – całość. W wyniku tego kilkadziesiąt terminów, każdy z innym podejściem, rozrastało się przez lata. Około 1980 r. połączyły się w kompleksowy, wspólny termin łączący pojęcie informacji i społeczeństwa: ta nowa koncepcja zawierała wszystkie poprzednie koncepcje częściowe, a nawet zachowywała ekspresyjną siłę, podejście i postawę, które reprezentowały[3].

W literaturze przedmiotu, zmiany procesów gospodarczych, ekonomicznych, społecznych i politycznych zachodzących na skutek zwiększenia tempa przepływu informacji są określane jako „rewolucja informacyjna". W zależności od podejścia metodologicznego i podmiotu badań początek rewolucji informacyjnej jest datowany pomiędzy latami 60. XX wieku, a początkiem lat 90. XX wieku.

1 S. Buregwa-Czuma, K. Garwol, *Definicje, właściwości i funkcje społeczeństwa informacyjnego*, „Dydaktyka informatyki" 2011, t. 6, s. 31.

2 http://paperroom.ipsa.org/papers/paper_64863.pdf.

3 L.Z. Karvalics, *Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression)*, Budapest 2007, s. 5–6.

Większość społeczeństw Europy znaczną część swojej działalności i aktywności przeniosła do sieci (komunikacja, bankowość elektroniczna, rozliczanie się z urzędami skarbowymi i dostęp do różnych baz danych). Również zarządzanie i sterowanie infrastrukturą odbywa się najczęściej poprzez internet. W związku z tym zapewnienie bezpieczeństwa cyfrowego społeczeństw jest jednym z kluczowych zadań władz państwowych. Funkcjonowanie społeczeństw informacyjnych, które w coraz większym stopniu są zależne od energii elektrycznej, opiera się na sieciach i systemach teleinformacyjnych. Powoduje to, że są one wyjątkowo podatne na zakłócenia, które mają wpływ na ich funkcjonowanie. Zagrożenia informatycznej strony funkcjonowania społeczeństw mają coraz poważniejsze konsekwencje, a ataki cybernetyczne mogą być wykorzystywane jako środek nacisku ekonomicznego i politycznego. W przypadku poważnych kryzysów działania w przestrzeni informatycznej mogą stanowić narzędzie oddziaływania uzupełniające tradycyjne siły zbrojne. Obecna era doświadcza nas szybszymi i rozleglejszymi zmianami niż kiedykolwiek w historii ludzkości. Ogrom informacji i eksplozja technologii informatycznych jest motorem napędowym, zmieniającym wszystkie aspekty życia społecznego, politycznego, kulturalnego i gospodarczego. Skutki rewolucji informacyjnej są szczególnie głębokie w zakresie strategii bezpieczeństwa narodowego.

Większość zjawisk i procesów politycznych ma swoje odzwierciedlenie w cyberprzestrzeni, a część z nich istnieje tylko w niej. Jednak źródła i przyczyny zjawisk społecznych (w tym politycznych) są umiejscowione poza przestrzenią wirtualną i wraz z procesami zachodzącymi przed erą internetu stanowią continuum. Dlatego w artykule zostały wykorzystane dwa podejścia badawcze. Pierwsze to zastosowanie metody instytucjonalno-prawnej, która polega na badaniu aktów normatywnych tworzonych przez instytucje[4]. Jej stosowanie wskazane jest przy badaniach systemów politycznych państw demokratycznych[5]. Metoda instytucjonalno-prawna może być stosowana

4 R. Żydok, *Przedmioty i metody badań politologicznych*, http://www.zydok.com/2008/01/przedmioty-i-metody-badan-politologicznych/#_ftn2.

5 R.M. Unger, *Legal Analisisas Institutional Imagination [w:]* R. Rawlings (red.), *Law, Society, and Economy: Centenary Essays for the London School of Economics and Political Science 1895–1995*, Oxford 1997, s. 177.

przy rozpoznawaniu stosunków międzynarodowych[6] oraz regulacji prawnych określających stosunki wewnątrzpaństwowe[7].

W artykule metoda instytucjonalno-prawna została użyta w celu zbadania ewolucji porządku prawnego Finlandii i Estonii w erze cyfryzacji oraz wpływy działań Federacji Rosyjskiej na te państwa.

Ponieważ głównym celem artykułu jest ukazanie Finlandii i Estonii w dobie zagrożeń hybrydowych (których składową są cyberwojna i cyberterroryzm), drugim podejściem badawczym jest podejście historyczne. Jest ono jednym z najczęściej stosowanych podejść badawczych w naukach politycznych[8]. Historia i nauki polityczne są ze sobą ściśle związane. Dziewiętnastowieczny angielski historyk, John Robert Seeley, stwierdził, że historia jest przeszłością polityki, a polityka jest teraźniejszością historii[9]. W wielu publikacjach opisujących metodologie badań w naukach politycznych przytoczone powyżej zdanie Freemana jest cytowane w kontekście uzasadniania użycia metody historycznej oraz opisywania politologii jako dziedziny naukowej[10]. Amerykański historyk i politolog Peter Charles Hoffer zaznacza, że podstawą zrozumienia każdego zjawiska będącego podmiotem badań politologicznych są wnikliwe badania nad historią tego zjawiska[11]. Również N. Jayapaln podkreśla, że dla zrozumienia ewolucji wszelkich zjawisk politycznych najistotniejsza jest znajomość historii[12]. Także Joseph W. Goodman podkreśla, że nawet przy opisywaniu takich zjawisk jak polityka telekomunikacyjna Unii Europejskiej, niezbędna jest dokładna analiza ich tła historycznego[13]. Leszek Moczulski w książce *Geopolityka. Potęga w czasie i przestrzeni* zaznacza, że zmienne układy przestrzenne

6 A. Chodubski, *Prognostyka jako wyzwanie metodologiczne w badaniu stosunków międzynarodowych*, Gdańsk 2009, s. 48.

7 J.S. Dryzek, *Discursive Democracy: Politics, Policy, and Political Science*, Cambridge 1994, s. 112.

8 T. Pawłuszko, *Wstęp do metodologii badań politologicznych. Skrypt akademicki*, Częstochowa 2013, s. 7.

9 G. Himmelfarb, *The New History and the Old: Critical Essays and Reappraisals. Revised Edition*, London 2004, s. 172.

10 C. Elman, M.F. Elman, *Introduction: Negotiating International History and Politics* [w:] C. Elman, M.F. Elman (red.), *Bridges and Boundaries: Historians, Political Scientists, and the Study of International Relations*, Cambridge 2001, s. 2–4.

11 P.C. Hoffer, *The Historians' Paradox. The study of History in Our Time*, New York 2008, s. 106–127.

12 N. Jayapalan, *Historiography*, New Delhi 2008, s. 10.

13 J.W. Goodman, *Telecommunications Policy-making in the European Union*, Norhampton 2006, s. 50.

nie odchodzą w przeszłość bez śladu[14]. Jednocześnie literatura określa układy przestrzenne w kategoriach gospodarczo-politycznych[15]. Podejście historyczne jest niezbędne dla zrozumienia genezy współczesnych zjawisk politycznych i zagrożeń hybrydowych ze strony Federacji Rosyjskiej, na jakie Estonia i Finlandia są narażone w szczególności.

Finlandia i Estonia wobec zagrożeń cyfrowych

Pierwszym państwem, które przekonało się, że korzyści płynące z cyberprzestrzeni idą w parze z nieznanymi wcześniej zagrożeniami była Estonia, najbardziej zinformatyzowane państwo świata, w którym obywatele mogli niemal wszystkie sprawy urzędowe załatwić online. W kwietniu i maju 2007 r. państwo to padło ofiarą skoordynowanych i zakrojonych na szeroką, niespotykaną wcześniej, skalę ataków cybernetycznych. Wydaje się uzasadnione twierdzenie, że Estonia stała się pierwszą ofiarą wojny cybernetycznej, w której jedno państwo sparaliżowało funkcjonowanie kluczowych instytucji i infrastruktury drugiego. Estonia mogła również stać się ofiarą testowania nowego rodzaju broni i taktyki wojennej. Pomimo braku (lub nieujawnianiu) jednoznacznych dowodów można przyjąć, że za tamtym atakiem stała Rosja. Wskazuje na to kontekst tamtych wydarzeń.

Estonia i Rosja mają długą historię sporów w stosunkach dwustronnych, a konflikty między etnicznymi Rosjanami i Estończykami sięgają setek lat przed powstaniem nowoczesnych państw narodowych. Po radzieckiej aneksji państw bałtyckich w 1940 r. i w czasie zimnej wojny Kreml przeniósł do Estonii setki tysięcy etnicznych Rosjan. Cel tych masowych migracji był dwojaki: zwiększenie spójności w bloku wschodnim i „zrusyfikowanie" kultury estońskiej. Po zakończeniu zimnej wojny i rozpadzie ZSRR, rząd w Tallinie wprowadził politykę mającą na celu minimalizację rosyjskich wpływów na kulturę estońską. Ataki cybernetyczne na Estonię miały miejsce w czasie, kiedy poziom napięcia między etnicznymi Estończykami a rosyjską mniejszością narodową osiągał apogeum. W dniu 30 kwietnia 2007 r. rząd Estonii przesunął Brązowego Żołnierza – pomnik upamiętniający radzieckie uwolnienie Estonii od nazistów – z Tõnismägi Park w centrum Tallina na cmentarz wojskowy w Tallinnie.

14 L. Moczulski, *Geopolityka. Potęga w czasie i przestrzeni*, Warszawa 2010, s. 316.
15 Ibidem, s. 317.

Ta decyzja wywołała zamieszki wśród rosyjskojęzycznej społeczności, która stanowiła w tamtym czasie około 26% populacji Estonii. Dla etnicznych Estończyków Brązowy Żołnierz symbolizował zniewolenie i ucisk. Ale dla mniejszości rosyjskiej przeniesienie to oznaczało dalszą marginalizację ich tożsamości etnicznej. Oprócz zamieszek i aktów przemocy, od 27 kwietnia do 18 maja, ataki DDoS (*Distributed Denial of Service*, rozproszona odmowa usługi) spowodowały zamknięcie stron internetowych wszystkich ministerstw, dwóch największych banków i kilku partii politycznych oraz parlamentarny serwer poczty elektronicznej. Estońscy urzędnicy, tacy jak minister spraw zagranicznych Urmas Paet, szybko oskarżyli Rosję o przeprowadzenie ataków, ale eksperci Komisji Europejskiej i NATO nie byli w stanie znaleźć wiarygodnego dowodu na udział Kremla w atakach DDoS[16].

Ataki na Estonię spowodowały szybką reakcję międzynarodową. W tamtym czasie państwo to nie posiadało odpowiednich służb przeciwdziałających cyberterroryzmowi i nie było przygotowane na ten typ ataku. Rządowy Zespół ds. Reagowania na Zagrożenia Cyfrowe (*ComputerEmergencyResponse Team* – dalej cyt.: CERT), aby przywrócić normalne operacje sieciowe, potrzebował pomocy ze strony partnerów fińskich, niemieckich, izraelskich i słoweńskich. Estoński CERT otrzymał również pomoc ze strony NATO. Co więcej, podczas kryzysu wśród państw zachodnich wystąpił wysoki poziom wymiany informacji wywiadowczych. Podczas gdy rosyjskojęzyczni hakerzy wykorzystali internet jako broń i narzędzie mobilizacji, Estonia i jej sojusznicy wykorzystali sieci cyfrowe, aby skutecznie przeciwdziałać atakom[17]. Po tamtych wydarzeniach władze Estonii podjęły szereg działań mających na celu zapobieżenie podobnym aktom terroru w przyszłości.

Estonia była jednym z pierwszych państw, które opracowały krajową strategię na rzecz bezpieczeństwa cybernetycznego (w 2008 r.). Zaktualizowana strategia została opublikowana w 2014 r. Obecnie Estonia posiada szeroki zakres ustawodawstwa obejmującego bezpieczeństwo informacji i cyberbezpieczeństwo. Estonia ma ugruntowany CERT pod kontrolą Urzędu Systemu Informacyjnego. Poza organami krajowymi, wpływ na bezpieczeństwo cyfrowe państwa ma fakt, że Centrum Doskonałości Bezpieczeństwa Cybernetycznego NATO (*CooperativeCyberDefence Centre of Excellence*, dalej cyt.: CCDCOE) mieści się w Estonii. Pomimo braku sformalizowanych partnerstw

16 S. Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, „Journal of Strategic Security" 2011, nr 2, s. 49–60.
17 Ibidem.

publiczno-prywatnych, w celu zwiększenia poziomu bezpieczeństwa cyfrowego, podmioty publiczne ściśle współpracują z odpowiednimi organizacjami sektora prywatnego[18].

We wszystkich swoich działaniach mających na celu zmniejszenie ingerowania Rosji w swoje sprawy wewnętrzne Estonia mogła liczyć na wsparcie i pomoc Finlandii. Finów i Estończyków łączy nie tylko bliskie pokrewieństwo etniczne i kulturowe, ale również poczucie zagrożenia ze strony Rosji. Aby zrozumieć obawy Finów należy przeanalizować tło historyczne stosunków fińsko-rosyjskich.

Po zakończeniu II wojny światowej, w przeciwieństwie do Estonii, Finlandia nie została zaanektowana przez Związek Radziecki i zachowała własną państwowość. Stała się jednak państwem zależnym od Moskwy zarówno pod względem polityki wewnętrznej, jak i zagranicznej. Przez cały okres powojenny rząd w Helsinkach próbował zachować równowagę pomiędzy niedawaniem Moskwie najmniejszego pretekstu do niezadowolenia, a nawiązywaniem stosunków ekonomiczno-gospodarczych z państwami zachodnimi[19]. Zwolennikiem prowadzenia takiej polityki był ówczesny prezydent Finlandii Juho Kusti Paasikivi, a po 1956 r. jego następca na urzędzie Urho Kaleva Kekkonen, który sprawował funkcję prezydenta aż do 1981 r. Zakładali oni, że Finlandia jest niepodległa tylko ze względu na swoje marginalne znaczenie dla Związku Radzieckiego. Znaczenie to mogło pozostać marginalne tylko dzięki unikaniu wszelkich układów międzynarodowych z państwami zachodnimi. Polityka taka, zwana później „finlandyzacją", była na początku nazywana linią polityczną Paasikivilego-Kekkonena[20]. Według fińskiego historyka, Jussi Hanhimäkiego, w okresie zimnej wojny Finlandia prowadziła jedną z najefektywniejszych polityk zagranicznych w Europie, która przeszła do historii jako „dyplomacja w saunie"[21]. Efektywna dyplomacja Helsinek pozwoliła Finlandii na integrację z Europą Zachodnią, pomimo długotrwałego znajdowania się tego państwa w radzieckiej strefie wpływów. Pomimo wielu kryzysów w stosunkach ze Związkiem Radzieckim, Finowie zdołali zachować niepodległość i równowagę w stosunkach politycznych, gospodarczych i kulturowych z państwami Europy

18 EU Cybersecurity Dashboard, *A Path to a Secure European Cyberspace*, http://cybersecurity.bsa.org/countries.html.

19 M. Jakobson, *Finland in the new Europe*, Westport 1998, s. 49.

20 F. Singleton, *The Myth of „Finlandisation"*, *„International Affairs"* 1981, nr 2.

21 M. Hanhimäki, *Security and Identity: the Nordic Countries and the United States since 1945* [w:] G. Lundestad (red.), *No End to Alliance: The United States and Western Europe: Past, Present and Future*, New York 1998, s. 87.

Środkowo-Wschodniej i Europy Zachodniej. Po upadku Związku Radzieckiego polityka Finlandii uległa reorientacji. Przyspieszył proces jej integracji ze strukturami gospodarczymi i militarnymi Europy Zachodniej.

Prawdopodobnie z obawy przed reakcją Moskwy Finlandia nie przystąpiła do NATO. Jednak nie oznacza to braku współpracy. Obecnie Finlandia jest jednym z pięciu państw (zwanych „partnerami o zwiększonych możliwościach"), które wnoszą szczególnie istotny wkład w operacje prowadzone przez NATO i wspierają inne cele Sojuszu. Dzięki temu ma ona zwiększone możliwości dialogu i współpracy z państwami sprzymierzonymi. W obecnym kontekście bezpieczeństwa międzynarodowego i rosnącymi obawami dotyczącymi rosyjskiej działalności wojskowej, NATO zacieśnia współpracę z Finlandią i Szwecją. Oznacza to poszerzenie dialogu politycznego, w tym na najwyższym szczeblu, wymianę informacji na temat wojny hybrydowej, koordynację szkoleń i ćwiczeń oraz rozwijanie wspólnej świadomości sytuacyjnej, aby w razie potrzeby przeciwdziałać wspólnym zagrożeniom i podejmować wspólne działania. Obydwa państwa uczestniczą we Wzmocnionych Siłach Odpowiedzi NATO (*NATO Response Force*, NRF), podlegając decyzjom krajowym, ale jednocześnie prowadzą regularne konsultacje z NATO w sprawie bezpieczeństwa w regionie Morza Bałtyckiego. W 2017 r. w Finlandii powstało Europejskie Centrum Doskonałości w Zakresie Zwalczania Zagrożeń Hybrydowych (*The European Centre of Excellence for CounteringHybridThreats*, dalej cyt.: HybridCoE) z siedzibą w Helsinkach. Centrum jest wspierane przez NATO i Unię Europejską[22]. Głównym celem powstania HybridCoE było stworzenie jednej instytucji koordynującej wykrywanie zagrożeń hybrydowych i reakcji na nie na poziomie UE i NATO. Obszary działania HybridCoE obejmują: 1) zachęcanie do dialogu i konsultacji na poziomie strategicznym między partnerami z UE i NATO; 2) wykrywanie działań hybrydowych skierowanych przeciwko zachodnim demokracjom przez podmioty państwowe i niepaństwowe oraz zwiększanie odporności partnerów na tego typu zagrożenia przez wykrywanie słabych punktów w ich systemach bezpieczeństwa; 3) przeprowadzanie szkoleń i organizowanie ćwiczeń opartych na scenariuszach mających na celu zwiększenie indywidualnych zdolności uczestników, a także interoperacyjności między uczestnikami UE i NATO w celu przeciwdziałania zagrożeniom hybrydowym; 4) prowadzenie badań i analiz zagrożeń hybrydowych oraz opracowywanie

22 NATO, *Relations with Finland*, https://www.nato.int/cps/en/natohq/topics_49594.htm?selectedLocale=en.

metod przeciwdziałania takim zagrożeniom; 5) tworzenie płaszczyzny współpracy dla ekspertów rządowych i pozarządowych mających na celu poprawę świadomości sytuacyjnej zagrożeń hybrydowych[23].

Obecnie aktywnie w działaniach HybridCoE uczestniczą UE, NATO oraz Czechy, Dania, Estonia, Finlandia, Francja, Włochy, Niemcy, Łotwa, Litwa, Holandia, Norwegia, Polska, Hiszpania, Szwecja, Wielka Brytania i USA. Uczestnictwo w działaniach Centrum jest otwarte również dla pozostałych państw członkowskich UE i NATO[24].

Współpraca Finlandii i Estonii w obszarze przeciwdziałania zagrożeniom cyfrowym

Stosunki Finlandii i Estonii charakteryzują się silnymi powiązaniami historycznymi i kulturowymi, a kontakty między tymi dwoma państwami są bardzo częste, wielopłaszczyznowe i wieloaspektowe. Niemal wszystkie estońskie ministerstwa ściśle współpracują z fińskimi. Dwustronna współpraca i kontakty pomiędzy estońskimi a fińskimi partnerami są szczególnie silne i częste w dziedzinie obrony, gospodarki, edukacji i badań, kultury, spraw wewnętrznych i wymiaru sprawiedliwości[25].

Obecnie szczególne miejsce we współpracy Estonii i Finlandii zajmują technologie informacyjne i komunikacyjne (*Information and Communication Technologies*, dalej cyt.: ICT). Państwa te ściśle współpracują w dziedzinie e-zarządzania i wymiany danych elektronicznych. Memorandum w sprawie cyfrowej współpracy Finlandii i Estonii zostało podpisane przez premierów Andrusa Ansipa (Estonia) i Jyrki Katainena (Finlandia) 10 grudnia 2013 r. Uzgodniono wówczas, że oba państwa będą współpracować w dziedzinie ITC i X-Road (X-Road to kluczowy element e-Estonii synchronizujący działanie państwowych i prywatnych e-serwisowych baz danych, platforma wymiany danych). Ustalono wówczas również, że Estonia i Finlandia będą wspólnie pracować nad dalszym rozwojem krajowej warstwy wymiany danych, tj. X-Road. Jesienią 2015 r. w Finlandii uruchomiono wersję testową platformy Palveluväylä (opartej na X-Road), która oferuje możliwość transgranicznego korzystania

23 Hybrid CoE, *About Us*, https://www.hybridcoe.fi/about-us/.
24 Ibidem.
25 Ministerstwo Spraw Zagranicznych Republiki Estonii, *Relations between: Finland*, http://vm.ee/en/countries/finland?display=relations#Co-operation.

z e-usług. W dniu 10 maja 2016 r. premierzy Taavi Rõivas (Estonia) i Juha Sipilä (Finlandia) podpisali wspólną deklarację o kontynuacji współpracy, która miała koncentrować się na uruchomieniu wymiany danych między obu państwami na podstawie platformy X-Road. Obecnie istnieją już rozwiązania techniczne, które umożliwiają wymianę danych między różnymi instytucjami Estonii i Finlandii za pośrednictwem X-Road. W czerwcu 2017 r. powołano Nordycki Instytut Rozwiązań Interoperacyjnych (*Nordic Institute for Interoperability Solutions*) do opracowania sposobu wymiany danych X-Road. Zostały utworzone specjalne kanały do realizacji transgranicznych usług elektronicznych z wymianą danych. Oba państwa współpracują przy uruchamianiu wymiany danych w następujących dziedzinach: dane rejestru ludności, dane z rejestru handlowego, recepty cyfrowe, dane o ubezpieczeniach społecznych, dane o ubezpieczeniach zdrowotnych oraz dane żeglugowe.

W dniu 7 lutego 2018 r. miała miejsce konferencja dotycząca pogłębienia współpracy pomiędzy obydwoma państwami. W konferencji brali udział ministrowie transportu Finlandii i Estonii oraz przedstawiciele samorządów z obu państw, a w czasie jej trwania przedstawiono studium wykonalności tunelu kolejowego łączącego Tallin i Helsinki (FinEst). Po zakończeniu studium wykonalności, estońskie Ministerstwo Spraw Gospodarczych i Komunikacji oraz fińskie Ministerstwo Gospodarki i Transportu utworzyły grupę roboczą, która określi kolejne etapy projektu tunelowego. Jednym z zadań grupy roboczej jest prowadzenie dalszych badań nad możliwością finansowania tej inwestycji. W trakcie swojej pracy grupa robocza weźmie pod uwagę wyniki i zalecenia z badania projektu FinEst. W świetle rozwoju technologicznego zostaną również rozważone dalekosiężne wpływy gospodarcze tunelu, opcje finansowania i kwestie dotyczące transportu i logistyki[26]. Tunel będzie mógł być również wykorzystany do budowy infrastruktury teleinformatycznej pozwalającej na bezpieczniejszą transmisją danych. Współpraca obronna między Estonią i Finlandią jest aktywna i obejmuje regularne konsultacje polityczne i wojskowe, a także praktyczne wspólne inicjatywy. Estonia i Finlandia podpisały umowę ramową o współpracy obronnej i na tej podstawie państwa kontynuują wymianę informacji na temat stanu bezpieczeństwa na Morzu Bałtyckim, planowania obrony, rozwoju zdolności wojskowych, badań i rozwoju w dziedzinie obronności, ćwiczeń szkoleniowych i cyberobrony. Oba państwa także ściśle współpracują w dziedzinie edukacji obronnej i szkolenia wojskowego,

26 Ibidem.

a także w dziedzinie wspólnych zamówień i kontroli zbrojeń. Od lat Finlandia wspiera Baltic Defense College (BALDEFCOL), wysyłając tam swojego instruktora[27]. Współpraca Finlandii i Estonii w misji UNIFL ONZ (tymczasowych sił Organizacji Narodów Zjednoczonych w Libanie) w Libanie rozpoczęła się w maju 2015 r., kiedy Estonia wniosła swój wkład wielkości plutonu piechoty do wspólnego batalionu Finlandii i Irlandii. Estoński pluton piechoty służy w zachodnim sektorze UNIFIL obok granicy z Izraelem, a jego głównym obowiązkiem było prowadzenie obserwacji i patroli oraz obsadzanie stanowisk kontrolnych. Członkowie Estońskich Sił Obronnych również współpracowali z siłami zbrojnymi Libanu. Wspólny batalion Finlandii i Irlandii przestanie działać pod koniec 2018 r. Finlandia uczestniczy w Centrum Doskonałości Bezpieczeństwa Cybernetycznej NATO z siedzibą w Estonii od października 2015 r. W centrum pracują dwaj fińscy eksperci. Estonia jest jednym z państw założycielskich Europejskiego Centrum Doskonałości do Zwalczania Zagrożeń Hybrydowych, które znajduje się w Finlandii[28].

Kolejnym przykładem na bliską współpracę Finlandii i Estonii w obszarze bezpieczeństwa było wspólne posiedzenie parlamentarnych komisji obrony Finlandii i Estonii. Najistotniejsze wnioski, jakie padły po tym wydarzeniu można wymienić w kilku punktach: 1) współpraca w dziedzinie obronności między państwami funkcjonuje dobrze; 2) brak członkostwa Finlandii w NATO nie jest przeszkodą w zacieśnianiu współpracy obronnej obu państw; 3) obok Szwecji, Stanów Zjednoczonych i Wielkiej Brytanii, Estonia jest dla Finlandii najważniejszym partnerem; 4) współpraca Finlandii i Estonii będzie się zaciskać dzięki wspólnym ćwiczeniom wojskowym i wspólnemu zakupowi sprzętu wojskowego.

W czasie spotkania potwierdzono zainteresowanie obu stron wzmocnieniem bezpieczeństwa w regionie Morza Bałtyckiego i Zatoki Fińskiej. Podkreślono również, że jednoczesna współpraca na poziomie Unii Europejskiej i NATO może zwiększyć poziom bezpieczeństwa partnerów znajdujących się we wspólnej przestrzeni informacyjnej. Członkowie narodowej komisji obronnej parlamentu Finlandii przedstawili przegląd planu rozwoju swojej armii i wydatków na obronę państwa, która zbliża się do poziomu 2% PKB ustalonego przez NATO[29].

27 Ibidem.
28 Ibidem.
29 Baltic News Service, *Defense committees of Estonian, Finnish parliaments hold joint meeting*. http://www.leta.lv/eng/defence_matters_eng/defence_matters_eng/news/1B718AD5-E90C-465F-86F7-03AC0ACF8D3F/.

Finlandia bierze udział również w corocznych ćwiczeniach cyberobrony organizowanych przez NATO CCD COE. Centrum organizuje największe na świecie i najbardziej złożone międzynarodowe ćwiczenia cyberbezpieczeństwa Locked Shields oraz doroczną konferencję na temat cyberkonfliktów CyCon. Sercem Centrum jest zróżnicowana grupa ekspertów – badaczy, analityków, szkoleniowców, edukatorów – z 20 krajów. Współpraca przedstawicieli sił zbrojnych, ekspertów rządowych i przedstawicieli przemysłu oznacza, że NATO CCD COE zapewnia unikalny, międzynarodowy 360-stopniowy ogląd współczesnego wymiaru cyberbezpieczeństwa[30].

Współpraca Finlandii i Estonii na płaszczyźnie bezpieczeństwa cyfrowego odbywa się również na płaszczyźnie niedostępnej dla opinii publicznej. Obecnie Estonia jest postrzegana jako najbardziej cyfrowe państwo świata, a przez to najbardziej narażona na zagrożenia cyberatakami. Można postawić tezę, że również Finlandia wielokrotnie padała ofiarą ataków. Jednak prawdopodobnie większość z nich jest nieznana opinii publicznej. Fińskie służby raczej nie informują ani o swoich działaniach, ani o ich wynikach. Jeden z nielicznych komentarzy dotyczył ujawnionych włamań do systemu informatycznego Ministerstwa Spraw Zagranicznych Finlandii. Incydent ten miał miejsce kilka lat wcześniej, ale został wykryty dopiero w 2013 r. Jednak sekretarz stanu w MZS Peter Stenlund oświadczył jedynie: Sprawcy wiedzą, że my wiemy, kim oni są, i wystarczy[31]. Stąd też wniosek, że Finlandia jest atakowana równie często jak Estonia, jednak są to informacje utajnione. Drugą poszlaką takiego stanu rzeczy jest zacieśnianie współpracy w ramach ochrony przed cyberatakami tych państw. Nie bez znaczenia pozostaje również fakt, że zarówno Finlandia, jak i Estonia są postrzegane przez Moskwę jako rosyjski obszar wpływów.

Zakończenie

Przykład ataku cybernetycznego na Estonię z 2007 r. udowodnił, że pierwszym elementem współczesnego konfliktu może być właśnie zniszczenie infrastruktury innego państwa przy pomocy narzędzi cyfrowych (oprogramowania). W niektórych przypadkach cyberataki mogą być skuteczniejsze od użycia klasycznych środków bojowych. Niewątpliwy postęp w dziedzinie

30 NATO CCD COE, *About Cyber Defence Centre*, https://ccdcoe.org/about-us.html.
31 TVP INFO, *Obce rządy przeprowadziły atak cybernetyczny na fińskie MSZ*, https://www.tvp.info/15888554/finlandia-msz-bylo-szpiegowane-przez-lata.

przeciwdziałania cyberatakom idzie w parze z doskonaleniem się grup przestępczych i terrorystycznych w tym obszarze. Dlatego w przypadku każdego państwa jest istotne stworzenie skutecznych procedur przeciwdziałania atakom cyfrowym. DDoSowy atak z 2007 r. był w gruncie rzeczy dość prymitywny i łatwy do wykrycia. O wiele niebezpieczniejsze są trudne do wykrycia działania wywiadowcze (jak to miało miejsce w przypadku szpiegowania MSZ Finlandii). Jednak żadne z działań służb zapewniających cyberbezpieczeństwo państwa nie powinno być upublicznione. Zagrożenia wynikające z powszechnego stosowania technologii informacyjnych nie dotyczą tylko państwa w znaczeniu instytucjonalnym. Z nowoczesnych technologii korzystają w życiu codziennym mieszkańcy niemal wszystkich państw świata. Jednocześnie większość urządzeń podłączonych do internetu nie posiada skutecznych zabezpieczeń przed złośliwym oprogramowaniem. Większość urządzeń mobilnych posiada wbudowane kamery, a aplikacje szpiegujące są powszechnie dostępne. Powoduje to potencjalną możliwość szpiegowania każdego w każdej sytuacji; nawet osób pełniących funkcje istotne dla bezpieczeństwa państwa. Jednocześnie w społeczeństwach sieciowych nie istnieje powszechna świadomość zagrożeń, jakie niesie za sobą korzystanie z urządzeń online. Wydaje się, że zarówno Estonia, jak i Finlandia znajdują się w obszarze zainteresowań służb Federacji Rosyjskiej. Mając tego świadomość państwa te starają się przeciwdziałać wrogiej aktywności.

Dotychczasowe tempo rozwoju technologii informacyjnych pozwala przypuszczać, że zagrożenia cybernetyczne mogą dotyczyć coraz większej części populacji i mieć coraz większy wpływ na funkcjonowanie państw. Aby temu przeciwdziałać państwa powinny ze sobą współpracować. Wydaje się, że działania takie zostały już zainicjowane po obu stronach Zatoki Fińskiej.

Bibliografia

Literatura

Buregwa-Czuma S., Garwol K., *Definicje, właściwości i funkcje społeczeństwa informacyjnego*, „Dydaktyka informatyki" 2011, t. 6.

Chodubski A., *Prognostyka jako wyzwanie metodologiczne w badaniu stosunków międzynarodowych*, Gdańsk 2009.

Dryzek J.S., *Discursive Democracy: Politics, Policy, and Political Science*, Cambridge 1994.

Elman C., Elman M.F., *Introduction: Negotiating International History and Politics* [w:] C. Elman, M.F. Elman (red.), *Bridges and Boundaries: Historians, Political Scientists, and the Study of International Relations*, Cambridge 2001.

Goodman J.W., *Telecommunications Policy-making in the European Union*, Norhampton 2006.

Hanhimäki M., *Security and Identity: the Nordic Countries and the United States since 1945* [w:] G. Lundestad (red.), *No End to Alliance: The United States and Western Europe: Past, Present and Future*, New York 1998.
Herzog S., *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, „Journal of Strategic Security" 2011, nr 2.
Himmelfarb G., *The New History and the Old: Critical Essays and Reappraisals. Revised Edition*, London 2004.
Jakobson M., *Finland in the new Europe*, Westport 1998.
Jayapalan N., *Historiography*, New Delhi 2008.
Karvalics L.Z., *Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression)*, Budapest 2007.
Moczulski L., *Geopolityka. Potęga w czasie i przestrzeni*, Warszawa 2010.
Pawłuszko T., *Wstęp do metodologii badań politologicznych. Skrypt akademicki*, Częstochowa 2013.
Unger R.M., *Legal Analisisas Institutional Imagination* [w:] R. Rawlings (red.), *Law, Society, and Economy: Centenary Essays for the London School of Economics and Political Science 1895–1995*, Oxford 1997.

Inne źródła

Baltic News Service, *Defense committees of Estonian, Finnish parliaments hold joint meeting*. http://www.leta.lv/eng/defence_matters_eng/defence_matters_eng/news/1B718AD5--E90C-465F-86F7-03AC0ACF8D3F/.
EU Cybersecurity Dashboard, *A Path to a Secure European Cyberspace*, http://cybersecurity.bsa.org/countries.html.
Hoffer P.C., *The Historians' Paradox. The study of History in Our Time*, New York 2008.
http://paperroom.ipsa.org/papers/paper_64863.pdf.
Hybrid CoE, *About Us*, https://www.hybridcoe.fi/about-us.
Ministerstwo Spraw Zagranicznych Republiki Estonii, *Relations between: Finland*, http://vm.ee/en/countries/finland?display=relations#Co-operation.
NATO CCD COE, *About Cyber Defence Centre*, https://ccdcoe.org/about-us.html (odczyt: 22.06.2018).
NATO, *Relations with Finland*, https://www.nato.int/cps/en/natohq/topics_49594.htm?selectedLocale=en.
Singleton F., *The Myth of „Finlandisation"*, „International Affairs"1981, nr 2.
TVP INFO, *Obce rządy przeprowadziły atak cybernetyczny na fińskie MSZ*, https://www.tvp.info/15888554/finlandia-msz-bylo-szpiegowane-przez-lata.
Żydok R., *Przedmioty i metody badań politologicznych*, http://www.zydok.com/2008/01/przedmioty-i-metody-badan-politologicznych/#_ftn2.

Prevention of digital threats on the example of the Republic of Estonia and the Republic of Finland

Abstract

The development of the telecommunication networks has caused social and political changes. Common access to the internet causes a large part of social activities to move to the virtual world. However, this universality has caused the emergence of new types of serious threats. Currently, terrorist attacks or warfare can be carried out remotely. Internationally important countries have their own services operating in cyber-space. Due to historical reasons and geopolitical location, Finland and Estonia are often treated

by the Kremlin as Russia's influence zones. In order to achieve its goals, the state puts pressure on countries that historically were parts of the Russian Empire using all possible means, including telecommunications networks. The flagship example of such action was the cybernetic attack on Estonia in 2007.

Key words: cybersecurity, NATO, Finland, Estonia, information society, telecommunication, terrorism, technological progress, information technology, Communications

Jacek Sobczak*

Przestępczość w cyberprzestrzeni między przepisami polskimi a międzynarodowymi

Streszczenie

W artykule podjęta jest problematyka przestępczości w cyberprzestrzeni, regulowanej za pośrednictwem przepisów krajowych oraz prawa międzynarodowego. W dobie społeczeństwa informacyjnego, gdzie internet posiada niezwykle duże znaczenie, a jego użytkowników ciągle przybywa, dochodzi do szeregu naruszeń prawa, które często stanowią przestępstwa. Przestępstwa w cyberprzestrzeni, rozumianej jako przestrzeń komunikacyjna tworzona przez system powiązań internetowych, stają się coraz groźniejsze i bywają coraz trudniejsze do wykrycia i ścigania.

Regulacje krajowe, jak też i międzynarodowe nie zawsze nadążają za dynamicznym postępem techniki, rozwojem sieci oraz wyzwaniami, które niesie ona za sobą. Nadal pojawiają się nowe czyny zabronione, popełniane w cyberprzestrzeni, w większym lub mniejszym stopniu sprzeczne z obowiązującym prawem, obnażające jednocześnie niedoskonałość przyjętych regulacji.

Słowa kluczowe: przestępczość, cyberprzestrzeń, społeczeństwo informacyjne, prawo krajowe, prawo międzynarodowe, zagrożenie, cyberterroryzm, cyberatak, system bezpieczeństwa

* Prof. dr hab. Jacek Sobczak, SWPS Uniwersytet Humanistycznospołeczny.

Zjawisko internetu

Pojawienie się internetu i objęcie siecią praktycznie całego świata nastąpiło stosunkowo niedawno, choć wyrosło już i nawet studiuje na wyższych uczelniach pokolenie, które ze zdziwieniem dowiaduje się, że były czasy, kiedy nie istniała sieć, podobnie jak kserokopiarki, skanery, ebooki itd. Założenia, które legły u podstaw internetu, będącego w istocie rzeczy zdecentralizowanym środkiem przekazu opartym na globalnej sieci połączeń, który składa się z wielu systemów komunikacyjnych, wykorzystywanych przez użytkowników, były wysoce idealistyczne. Stanowiły one bowiem próbę zbudowania nowego społeczeństwa o charakterze liberalnym, cieszącym się wolnością słowa – nieskomercjonalizowanego i niezależnego politycznie[1]. Wszelkie reguły działania internetu miały być oparte o *Netykietę* – dobrowolnie przyjmowaną i przestrzeganą przez użytkowników sieci[2]. Wróżby prawników, że prędzej czy później internet będzie musiał zostać poddany regulacjom prawnym większość internautów, w szczególności pochodzących ze środowisk informatyków przyjmowała je z niedowierzaniem i kwitowała pogardliwym wzruszeniem ra-

1 L.W. Zacher, *Etykietowanie przyszłych społeczeństw – kryteria, określenia, ewaluacje* [w:] M. Sokołowski (red.), *U progu wielkiej zmiany? Media w kulturze XXI wieku*, Olsztyn 2005, s. 23–34; Z. Łęski, Z. Wieczorek, *Społeczeństwo wirtualne – czy mamy jakiś wybór?* [w:] M. Sokołowski, M. Furmanek (red.) *Oblicza Internetu. Internet a globalne społeczeństwo informacyjne*, Elbląg 2005, s. 13–28, I. Korcz, *Internet a człowiek w kontekście globalizującego się świata?* [w:] M. Sokołowski, M. Furmanek (red.) *Oblicza…*, s. 29–34.

2 Eksploatowanie sieci komputerowych (w pierwszym rzędzie internetu) doprowadziło do wykształcenia się wielu swoistych zasad i zwyczajów, które nie zostały skodyfikowane i nie wszystkie są w jednakowej mierze aprobowane i przestrzegane. Mimo to jednak wiele z nich zyskało rangę szczególnych norm etycznych, składających się na to, co określa się jako „etyka sieci" (*Netiquette, Nethic, Cybermanners* – w języku polskim: *Netykieta).* Zob. A.H. Rinaldi, *Internationale Netze und das Wettberbstrecht* [w:] J. Becker (red.), *Rechtsprobleme internationalen Dattenetze*, Baden-Baden 1996, s. 13–35 i n. Tak więc, *Netykieta* to zasady etyczne regulujące zachowanie się w sieci. Nie ma ona jednak charakteru zbioru norm prawnych, gdyż nie formułuje jakichkolwiek sankcji za nieprzestrzeganie przyjętych zasad oprócz ostracyzmu użytkowników internetu. Najczęściej przyjmowana jest angielska wersja *Netykiety*, znana jako dokument RFC 1855 (*Netiquette Guidelines).* Znana jest w wielu innych wersjach i odmianach. Wskazać należy wśród nich dokument napisany przez Arlene H. Rinaldi z Florida Atlantic University w 1992 r. Zob. http://tools.ietf.org/html/rfc1855; http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/10.Commandments.html. W odniesieniu do działalności reklamowej w internecie Międzynarodowa Izba Handlowa wypracowała szczególne zasady postępowania, mające jednak również charakter norm etycznych, a mianowicie *Guidelines on Interactive Marketing Communications*, zob. T. Hoeren, *Werberecht im Internet am Beispiel der ICC Guidelines on Interactive Marketing Communications* [w:] M. Lehmann (red.), *Internet – und Multimediarecht (Cyberlaw)*, Stuttgart 1997, s. 112 i n.

mion. Wkrótce jednak okazało się, iż internet, wraz z rozszerzaniem się sieci, powiększaniem się liczby użytkowników, tracił przysłowiową „niewinność". Wśród jego użytkowników miejsce intelektualistów zaczęli zajmować biznesmeni, a w końcu stał się on podstawowym narzędziem, bez którego nie mogą już się obejść miliony, a nawet miliardy zwykłych ludzi. Spowszednienie internetu spowodowało także i to, że zaczęto poszukiwać w jego zasobach treści mniej wysublimowanych, a nawet całkowicie przaśnych, takich jak informacje handlowe, gospodarcze, usługowe[3], polityczne[4], a nawet o charakterze erotycznym.

Rewolucja informacyjna, efektem której był szybki rozwój i upowszechnienie się światowej sieci (efekt informatyczny), zmieniła oblicze współczesnego świata. Wpłynęła na styl życia jednostki, zmieniła sposób funkcjonowania społeczeństwa (efekt socjologiczno-psychologiczny) oraz zredefiniowała rolę państwa (efekt polityczno-prawny). Transformacja stosunków społecznych wpłynęła na zmianę systemów gospodarczych, rozwinęły się nowe wirtualne dziedziny zarówno związane z handlem, jak i finansami. Konsekwencje tych przemian są również widoczne w obszarze bezpieczeństwa.

Możliwość docierania za pośrednictwem internetu do praktycznie nieograniczonej liczby odbiorców zwróciła nań uwagę kół przemysłowo-handlowych, które dostrzegły możliwość wykorzystywania jego potencjału do komunikacji z klientami. Internet okazał się doskonałym narzędziem marketingowym oferującym bogatą gamę usług reklamowych i informacyjnych. Posługiwanie się internetem, w szczególności pocztą elektroniczną przez polityków, przedsiębiorców, handlowców i podmioty świadczące usługi doprowadziło do tego, że odbiorca poczty elektronicznej znalazł się rychło w sytuacji odbiorcy korzystającego z usług poczty tradycyjnej. Podobnie jak ten drugi został zasypany dziesiątkami, potem setkami i tysiącami nigdy niezamawianych reklam, anonsów i ogłoszeń, wśród których ginęły informacje naprawdę dla niego ważne i oczekiwane. Coraz więcej czasu każdy z użytkowników musi poświęcać na segregowanie informacji, na pozbywanie się niechcianej korespondencji. Praktyka taka dotyczy w pierwszym rzędzie reklam o charakterze gospodarczym. Zachęcają mniej lub bardziej nachalnie do nabycia określonych towarów lub skorzystania z określonych usług. Pojawiają się jednak także – i to dość licznie –

3 P. Bickerton, M. Bickerton, U. Pardesi, *Marketing w internecie*, Gdańsk 2006, szczególnie s. 21–151.

4 A. Turska, *Marketing polityczny w Internecie* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006, s. 199–211.

przekazy o charakterze politycznym[5], społecznym bądź religijnym[6], nakłaniające do głosowania na tego czy innego polityka, poparcia partii politycznej[7], określonych idei, czy programów, względnie przyjęcia pewnych dogmatów religijnych[8]. Przyznać jednak należy, że zwłaszcza w rzeczywistości polskiej przekazy internetowe tego ostatniego typu mają charakter marginalny i ich uciążliwość dla odbiorcy jest relatywnie mniejsza. Oczywiście, wspominając o dolegliwości należy mieć na względzie przeciętnego odbiorcę treści reklamowych, skoncentrowanego na własnych problemach i niezainteresowanego informacjami, których w danym momencie nie poszukuje.

Niestety w sieci pojawiło się szereg zjawisk niezwykle groźnych, niebezpiecznych, godzących w prawa i wolności człowieka, naruszających jego prywatność, godność, dobre imię i cześć, wymierzone w tajemnicę środków przekazu, zasadzające się na nieuprawnionym dostępie do informacji bądź do całości lub części systemu informacyjnego, objawiające się w nielegalnym podsłuchu oraz w inwigilacji przy użyciu urządzeń technicznych i programów komputerowych, ujawnianych informacji uzyskanych nielegalnie. Przy wykorzystaniu internetu można naruszać integralność zapisu informacji, bądź danych, utrudniać do nich dostęp sabotować przekaz, zakłócać pracę systemów komputerowych by sprawnie wykorzystywać urządzenia, programy i dane, naruszać korespondencje itd. Za pośrednictwem internetu mogą i są

5 S. Sobczyk, *Internet narzędziem oddziaływania na wyborców* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006, s. 109–116; H. Kotarski, *Internet a lokalna polityka. Studium socjologiczne na przykładzie wyborów samorządowych* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006, s. 117–124; G. Schittek, *Internet jako narzędzie politycznego wsparcia w Szwecji* [w:] T. Zasępa (red.), *Internet. Fenomen społeczeństwa informacyjnego*, Częstochowa 2001, s. 219–226.

6 T. Zasępa, *Komunikacja cybernetyczna wyzwaniem dla Kościoła katolickiego* [w:] T. Zasępa (red.), *Internet i nowe technologie – ku społeczeństwu przyszłości*, Częstochowa 2003, s. 51–54.

7 A. Kasińska-Metryka, *Demokratyzacja systemu politycznego a przepływ informacji – od deficytu do przesytu* [w:] M. Sokołowski (red.), *U progu…*, s. 107–114; P. Gulda, *Elektroniczna demokracja – teoria i praktyka, wady i/lub zalety* [w:] M. Sokołowski (red.), *U progu…*, s. 115–121; P. Gulda, *Internet jako przestrzeń polityczna* [w:] M. Sokołowski (red.), *Edukacja medialna. Nowa generacja pytań i obszarów badawczych*, Olsztyn 2004, s. 47 i n.; M. Boszczyk, *Media elektroniczne jako środek komunikowania politycznego* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym*, Sosnowiec 2006, s. 180–198.

8 W. Muszyński, *Wizerunek polskich tradycjonalistów katolickich w Internecie* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI*, Elbląg 2006, s. 261–278; A. Korzińska, *Tradycja i nowoczesność. Islam w Internecie. Analiza polskojęzycznych stron internetowych* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI*, Elbląg 2006, s. 279–286.

przekazywane treści pornograficzne, upowszechnia się zjawisko pedofilii oraz rozpowszechniany jest wyjątkowo okrutny „język nienawiści”[9]. Pojawiło się też jeszcze groźniejsze zjawisko w postaci cyberterroryzmu, godzące podstawy funkcjonowania demokratycznych państw i społeczeństw, bezpieczeństwo stosunków międzynarodowych, wolność wyborów politycznych w różnych państwach, rozmontowujące, oparte na systemach komputerowych, systemy porozumiewania się, bądź przesyłania energii. Niektóre z tego rodzaju czynów godzą wprost w bezpieczeństwo publiczne, gdyż wymierzone są w funkcjonowanie sił zbrojnych, aparatu bezpieczeństwa państwa, a nadto zmierzają do wywołania paniki publicznej[10].

9 R. Wieruszewski, M. Wyrzykowski, A. Bodnar, A. Gliszczyńska-Grabias, *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010, passim; K. Grzybczyk, *Twórczość internautów w świetle regulacji prawa autorskiego na przykładzie fanfiction*, Warszawa 2015, passim; L.K. Jaskuła, *Wolność działalności dziennikarskiej w perspektywie zjawiska mowy nienawiści. Wybrane aspekty prawne* [w:] W. Lis (red.), *Status prawny dziennikarza*, Warszawa 2014; M. Woiński, *Prawnokarne aspekty zwalczania mowy nienawiści*, Warszawa 2014, passim.

10 M. Gołda-Sobczak, *Spór o definicję terroryzmu*, „Wiedza i Umiejętności” 2004, t. 5, s. 47–63. Alex Schmid dysponując niewątpliwie niepełnymi danymi, bazując głównie na literaturze amerykańskiej i anglojęzycznej, wyliczył ponad sto rozmaitych definicji terroryzmu, nie znajdując wśród nich żadnej zadowalającej. Podobne stanowisko prezentował Walter Laqueur. Zob. A.P. Schmid, *Political Terrorism: A Research Guide*, New Brunswick 1984, s. 10; W. Laqueur, *Terrorism*, London 1997, s. 7; W. Laqueur, *The Ageof Terrorism*, Boston 1987, s. 11. W praktyce istnieje wiele definicji terroryzmu, które zdaniem K. Indeckiego można podzielić ze względu na kryterium ujmowanego przez nie zakresu przedmiotowego na trzy grupy: generalne, cząstkowe oraz mieszane. Własne definicje terroryzmu przedstawili między innymi: T. Hanusek, *W sprawie pojęcia współczesnego terroryzmu*, „Problemy Kryminalistyczne” 1980, nr 143; M. Fleming, *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy”1996, nr 1; S. Pikulski, *Prawne środki zwalczania terroryzmu*, Olsztyn 2000; T. Aleksandrowicz, *Współczesny terroryzm międzynarodowy – próba definicji ze stanowiska prawa międzynarodowego*, „Wojskowy Przegląd Prawniczy” 2003, nr 2; K. Indecki, *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź 1998, s. 19–22. Zob. także: B. Hoffman, *Oblicza terroryzmu*, Warszawa 2001, s. 13–15; tamże ciekawe nawiązanie do stanowiska W. Laqueur, *The Age of Terrorism*, Boston 1987, s. 11. Zob. A Pawłowski, *Terroryzm w Europie w XIX i XX wieku*, Zielona Góra 1980, s. 9. Zjawisko terroryzmu zaczęto analizować jako rodzaj ukrytej lub zastępczej wojny pozwalającej słabszym państwom na konfrontacje z silniejszymi rywalami. Zob. C. Sterling, *Śmierć terroru: prawda o międzynarodowym terroryzmie*, przeł. M. Fogg i E. Petrajtis-O’Neill, Warszawa 1990. Zob. także: R.S. Cline, *Yonah Alexander: The Soviet Connection*, New York 1984, J. Becker (red.), *The Soviet Union and Terrorism*, London 1984. Na konotacje te zwrócił uwagę B. Hoffman, s. 24–25. Termin *terroryzm* niektórzy odnosili do wszystkich działań czynników niepaństwowych i pozarządowych destabilizujących określone regiony lub terytoria miejskie. Terroryzm stał się też wygodnym określeniem pozwalającym na objęcie jego zakresem wszelkich konfliktów współczesnego świata, które nie przystawały do tradycyjnego obrazu wojny toczonej przez regularne armie dwu lub kilku państw. Zob. B. Hoffman, *Low-intensity Conflict: Terrorism and Guerrilla War*

Narodom Europy, w toku wielowiekowych, okupionych śmiercią i cierpieniem wielu ludzi, udało się osiągnąć zakaz cenzury prewencyjnej, zniweczyć kontrole prasy, publikacji, widowisk. Stało się to jednak w momencie, kiedy „tradycyjna" wymiana informacji, ograniczona do prasy, radia, telewizji, książek i spektakli, zaczęła odgrywać coraz mniejszą rolę, a jej znaczenie powoli malało pod wpływem internetu umożliwiającego zdecydowanie szybszą wymianę myśli – lecz także dającemu większe możliwości kontroli treści przekazu. Nagłaśniane przez prasę, często demonizowane niebezpieczeństwa terroryzmu oraz pedofilii pojawiły się jakby na zamówienie władz publicznych, jako dogodny pretekst do rozpoczęcia kontroli treści przekazywanych informacji. Tym samym, władzom państw uznającym się za demokratyczne (i tak traktowanych przez ogół) udało się to, co nie powiodło się reżimom totalitarnym, to, co okazuje się być marzeniem tyranów, władców absolutnych, dyktatorów – kontrola myśli i uczuć obywateli, poznanie ich prawdziwego „ja"[11].

fare in the Coming Decades [w:] L. Howard (red.), *Terrorism: Roots, Ompact, Responses, Praegor*, New York 1992, s. 140. W myśl decyzji ramowej z 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.Urz. UE L 2002, nr 164, s. 3) zobowiązano państwa unijne do przyjęcia zbliżonych definicji przestępstw terrorystycznych. Wspomniana decyzja ramowa została zastąpiona dyrektywą Parlamentu Europejskiego i Rady UE 2017/541 z dnia 15 marca 2017 w sprawie zwalczania terroryzmu i zastępującą decyzję ramową 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW (Dz.Urz. UE L 2017, nr 88, s. 6). W systemie prawnym Rady Europy opracowano Konwencję Rady Europy o zwalczaniu terroryzmu (Dz.U. z 1996, nr 117, poz. 557) w systemie uniwersalnym opracowano Konwencję o zwalczaniu ataków terrorystycznych z użyciem bomb z 15 grudnia 1997 r. oraz międzynarodową Konwencję o zwalczaniu finansowania terroryzmu z dnia 9 grudnia 1999 r. (Dz.U. z 2004, nr 263 poz. 2620). Por. J.W. Wójcik, *Przeciwdziałania finansowaniu terroryzmu*, Warszawa 2007, s. 131–152. Zgodnie z regulacją zawartą w art. 115 § 20 k.k. „przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: poważnego zastraszenia wielu osób; zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności; wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu".

11 Zob. J. Sobczak, *Wolność słowa a zjawisko inwigilacji przekazu internetowego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Architektura komunikacyjna sieci*, Elbląg 2007, s. 71–94.

Społeczeństwo informacyjne

Dążenie do społeczeństwa informacyjnego będące skutkiem procesów globalizacyjnych przebiega nieco inaczej w Europie na obszarze Unii Europejskiej i Rady Europy oraz w Stanach Zjednoczonych i Japonii[12].

Po raz pierwszy wizja społeczeństwa informacyjnego pojawiła się w 1993 r. w opublikowanej przez Komisję Europejską białej księdze pod tytułem *White Paper on Growth, Competitiveness, Employment. The Challenge and way forward into 21st century*[13]. Przedstawione w białej księdze społeczeństwo informacyjne miało być wielką szansą dla Europy, dlatego podkreślano w niej jego pozytywne ekonomiczne i społeczne rezultaty dla gospodarki, niewiele miejsca poświęcając negatywnym skutkom informatyzacji. Podstawowym celem strategicznym, związanym z budową społeczeństwa informacyjnego, miała być całkowita liberalizacja sektora telekomunikacji, która oprócz pobudzenia konkurencji w tej dziedzinie, poprzez przykładowo wprowadzenie nowych operatorów, miała stanowić podłoże do utworzenia europejskiego rynku usług i produktów informacyjnych. Założenia białej księgi zostały skonkretyzowane w dokumencie *Europe and the Global Information Society: recommendations to the European Council* (Europa a społeczeństwo globalnej informacji), zwanym Raportem Bangemanna, opublikowanym w 1994 r.[14] Raport stanowił podstawę do opracowania szczegółowych planów działań, obejmujących tworzenie nowych aktów prawnych i różne inicjatywy, finansowane ze środków publicznych Unii Europejskiej. Dokument otworzył publiczną debatę na temat europejskich szans zrównoważonego rozwoju, wzmocnienia gospodarki, aktywnego konkurowania na rynkach światowych. Raport Bangemanna odzwierciedlał

12 J. Sobczak, *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała, J. Iwanek, *Demokracja w dobie globalizacji*, t. II, *Aspekty teoretyczne*, Katowice 2008, s. 52–79; J. Sobczak, *Problemy społeczeństwa informacyjnego w dobie globalizacji* [w:] T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007, s. 193–213; J. Sobczak, *Europejski ład komunikacyjny w procesie globalizacji* [w:] J. Sobczak, R. Bäcker, *Europejska myśl polityczna wobec globalizacji*, Łódź 2005, s. 39–70. Zob. także: K. Doktorowicz, *Europejska droga do społeczeństwa informacyjnego* [w:] K. Doktorowicz (red.), *Społeczeństwo informacyjne. Wyzwania dla gospodarki, polityki i kultury*, Katowice 2002, s. 75 i n.

13 *White Paper on Growth, Competitiveness, Employment. The Challenge and way forward into 21st century*, COM (93) 700 final.

14 Raport *Recommendations to the European Council, Europe and the global information society* został opublikowany przez Komisarza do spraw Społeczeństwa Informacyjnego Unii Europejskiej Martina Bangemanna w 1994, http://europa.eu.int/ISPO/infosoc/backg/bangeman.html.

optymistyczny punkt widzenia przedstawiony w białej księdze i znacząco przyczynił się do aktywizacji wielu środowisk zawodowych i społecznych widzących w technologiach teleinformatycznych szansę dla Europy[15].

Kolejnym ważnym dla rozwoju społeczeństwa informacyjnego dokumentem europejskim była zielona księga Komisji Europejskiej *Living and Working in Information Society. People First* (Życie i praca w społeczeństwie informacyjnym. Człowiek na pierwszym miejscu) z 1996 r.[16] Dokument ten był wyrazem zmian w polityce europejskiej, gdzie priorytetem stały się cele społeczne. Zielona księga koncentrowała się na problematyce społecznej i socjalnej, w tym przede wszystkim na zatrudnieniu oraz budowie społecznej solidarności, równych szans i kulturalnej różnorodności Europy. W styczniu 1999 r. opublikowano kolejną zieloną księgę, zatytułowaną *Public Sector Information in the Information Society* (Zielona Księga na temat Informacji Sektora Publicznego w Społeczeństwie Informacyjnym)[17]. Poruszała ona głównie zagadnienia powszechnego dostępu, kładąc nacisk na wykorzystanie infrastruktury informacyjnej do realizacji fundamentalnych praw człowieka, takich jak wolność informacji czy też prawo do informacji. Podsumowując europejskie wysiłki podejmowane w latach 1993–1999 w celu budowania społeczeństwa informacyjnego, należy podkreślić, iż koncentrowały się one na trzech priorytetach: tworzenie środowiska industrialnego i biznesowego, pozwalającego na inwestowanie w infrastrukturę informacyjno-komunikacyjną, polityka innowacyjności oraz dialog społeczny prowadzący do akceptacji zmian i uczestnictwa w zmianach[18].

Pojęcie cyberprzestrzeni

Pojęcie „cyberprzestrzeni" jest terminem, który narodził się w obszarze dość odległym od prawa, bo w powieści *Burning Chrome*, będącej pierwszym tomem trylogii *Neuromancer* autorstwa Williama Gibsona, amerykańskiego pisarza science fiction. Równolegle pisarz posługiwał się jednak terminem „matrix" – matryca. Spopularyzowały cyberprzestrzeń filmy opierające się na motywach

15 J. Sobczak, *Dylematy społeczeństwa informacyjnego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI wieku*, Elbląg 2006, s. 13–36.
16 *Living and Working in Information Society. People First*, COM (96) 389 final.
17 *Green Paper on Public Sector Information in the Information Society*, COM (99) 585 final.
18 K. Doktorowicz, *Europejski model społeczeństwa informacyjnego*, Katowice 2005, s. 177.

wspomnianej trylogii, a mianowicie *Matrix* i *Johny Mnemonic*[19]. Do powszechnego użytku określenie „cyberprzestrzeń" wchodzi w początkach lat 90. wraz z rozwojem technologii informacyjnych. Uznaje się ją za ściśle związaną z globalizacją[20] i powstaniem społeczeństwa informacyjnego[21]. Odtąd definiowana

19 Zob. w tej kwestii A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, nr 3, s. 6.

20 Terminem globalizacja chętnie posługują się zarówno uczeni, jak i publicyści, usiłując za jego pomocą wyjaśnić zjawiska i procesy, których widownią stał się świat na przełomie XX i XXI w. Podkreśla się przy tym, że globalizacja stanowi końcowy etap historycznej transformacji i elektronicznie przekazywanej kultury popularnej, połączonej z propagowaniem ideologii liberalnej przez rozwinięte państwa demokratyczne. Przegląd definicji pojęcia globalizacja i próbę ich systematyzacji przynosi praca K. Gilarka, *Państwo narodowe a globalizacja – dynamika powstawania nowego ładu*, Toruń 2003, s. 39–46. Por. także: N. Stammers, *Social movements and the challenge to power* [w:] M. Shaw (red.), *Politics in Globalized Word*, London 1999, s. 73 i n.; J.A. Scholte, *The Globalization of World Politics* [w:] J. Baylis, S. Smith (red.), *The Globalization of World Politics. An Introduction to International Relations*, New York 2001, s. 23; J.A. Scholte, *Globalization: prospects for a paradigm shift* [w:] *Politics in Globalized*, s. 9 i n.; I. Clark, *Globalization and International Relation Theory*, Oxford 1999, s. 35. Opisując je zwraca się zwykle uwagę na jego wymiar polityczny, gospodarczy i militarny zapominając, że u jego podstaw leży ważniejszy chyba wymiar kulturowy, któremu sprzyja nowoczesna technika. W literaturze trwa spór o początek procesów globalizacji, a także o to, jaka jest istota tego procesu lub procesów. W tym względzie por. W. Anioł, *Geneza i rozwój procesów globalizacji*, Warszawa 1989, passim; Z. Barman, *Globalizacja*, Warszawa 2000, s. 5–10. Termin „globalizacja", jak przyjmuje się w literaturze, najprawdopodobniej pojawił się po raz pierwszy w słowniku Webstera z 1961 r. Według R. Kilminstera, jest to moment, od którego zaczęto w nauce dostrzegać, iż wydarzenia polityczne i militarne oraz relacje społeczne mają ciągle wzrastające znaczenie nie tylko dla obszaru, na którym zaistniały, lecz także w skali całego globu. W kwestii globalizacji por. także: M. King, *Globalization, Knowledge and Society*, New York 1990. Sporne jest także i to, czy globalizacja jest wynikiem jednego procesu, czy też wypadkową kilku lub kilkunastu tendencji. Stanowiska prezentowane w tym względzie dotyczące istoty i zakresu procesów globalizacji przedstawił M. Pietras, *Globalizacja jako proces zmian społeczności międzynarodowej* [w:] M. Pietras (red.), *Oblicza procesów globalizacji*, Lublin 2002, s. 36–50.

21 Termin „społeczeństwo informacyjne" to określenie stosunkowo młode. Jako pierwszy miał się nim posłużyć w 1963 r. Tadao Umesao, pisząc o japońskiej gospodarce zdominowanej przez informacje i technologie i zastanawiając się nad ewolucyjną teorią społeczeństwa opartego na przemysłach informacyjnych. Określenie to zostało następnie spopularyzowane przez Kenichi Koyamę w rozprawie *Introduktion to Information Theory* w 1968 r. Do Europy koncepcja społeczeństwa informacyjnego zawitała w 1978 r., kiedy to Simon Nor i Allain Minc omówili ją w raporcie przedstawionym prezydentowi Francji. Nieco później, bo w początkach lat osiemdziesiątych, koncepcja społeczeństwa informacyjnego dociera do USA, robiąc w tamtejszych ośrodkach naukowych zawrotną karierę. T. Goban-Klas, *Społeczeństwo informacyjne i jego teoretycy* [w:] J. Lubacz (red.), *W drodze do społeczeństwa informacyjnego*, Warszawa 1990, s. 29–30. Koncepcja społeczeństwa informacyjnego nie pojawiła się, co oczywiste, w próżni intelektualnej wpisuje się ona w ten nurt refleksji socjologiczno-politologicznej, które starają się zdefiniować i scharakteryzować współcześnie istniejące zbiorowości. Wydaje się, iż u źródeł koncepcji społeczeństwa informacyjnego leży nurt determinizmu technologicznego oraz ewolucjonizmu naukowego, którego zwolennicy

jest jako przestrzeń komunikacyjna tworzona przez system powiązań

zafascynowani zdobyczami technologicznymi podkreślali, że wymuszają one fundamentalne i nieodwracalne zmiany w kulturze i instytucjach społecznych. U podstaw tej koncepcji leży także niewątpliwie teoria modernizacji M. Webera, widzącego w biurokracji nieuchronną, wręcz metafizyczną siłę napędową współczesnego świata. Por. M. Weber, *Gospodarka i społeczeństwo. Zarys socjologii rozumiejącej*, Warszawa 2002, s. 693–726; por. także: S. Andreski, *Maksa Webera olśnienia i pomyłki*, Warszawa 1992, s. 67 i n. Zarówno determinizm technologiczny, jak i weberowska teoria biurokratycznej modernizacji wraz ze skonstatowaną, w płaszczyźnie historycznej, rewolucją przemysłową doprowadziły do wykształcenia koncepcji społeczeństwa przemysłowego (industrialnego), które miało się cechować wykształconą organizacją państwową, komercjalizacją produkcji masowej, wysokim stopniem uprzemysłowienia oraz zatrudnieniem większości członków społeczeństwa poza sektorem rolniczym. Wraz z mechanizacją i rozwojem technicznym podnoszącym standard życia miało nastąpić zniesienie struktur klasowych i zastąpienie ich przez bardziej zróżnicowane i mniej spolaryzowane systemy stratyfikacji zawodowej. Polityczną konsekwencją miał być pluralizm, rozproszenie władzy, koniec rządów autorytarnych Por. C. Kerr, J.T. Dunlap, F.H. Harbison, C.A. Myers, *Industrialism and Industirial Man*, Cambridge 1960. Koncepcja społeczeństwa przemysłowego prowadziła do teorii społeczeństwa postprzemysłowego, czyli takiego, w którym wiedza zastępuje własność, stając się głównym przedmiotem zabiegów oraz najważniejszym źródłem władzy i dynamizmu społecznego. Miało to być społeczeństwo, w którym głównym miejscem zatrudnienia ludności staje się sektor usług, w szczególności w płaszczyźnie finansów, ubezpieczeń, zdrowia, nauki i oświaty. Twórca tej koncepcji, Daniel Bell, podkreślał, iż dominować w społeczeństwie postprzemysłowym będą specjaliści i naukowcy, a wiedza teoretyczna będzie miała centralne znaczenie, jako źródło innowacji i polityki. Wieścił on także coraz szerszy zakres kontroli społecznej rozwoju techniki oraz tworzenie „technologii intelektualnych", jako podstawy podejmowania decyzji politycznych i społecznych. Por. D. Bell, *The Coming of Post-Industial Society*, New York 1973; wyd. II Harmondsworth 1976. W kolejnych prawach Bell posługiwał się już terminem „społeczeństwo informacyjne", wskazując, że jego cechą charakterystyczną jest wzrost produkcji i przepływu informacji wszelkiego rodzaju. Zdawał sobie jednak sprawę z tego, że ma ono charakter w gruncie rzeczy modelu idealnego, a nie realnego. Pomijając w tym miejscu treść jego wywodów odnoszących się do problematyki zmian społecznych, które miały stymulować powstanie społeczeństwa postindustrialnego oraz jego neoewolucyjnego spojrzenia na historię, wypada podkreślić, że o ile w społeczeństwie przedindustrialnym życie jest walką z przyrodą, to w erze industrialnej bój toczy się przeciwko przetworzonej przyrodzie. W epoce przedindustrialnej dominuje siła człowieka. Następująca po niej era industrialna to okres supremacji maszyny. W następnym okresie, w dobie społeczeństwa postindustrialnego, liczy się już tylko informacja. Wyróżnił w ten sposób D. Bell trzy rodzaje pracy: wydobywczą, fabryczną oraz informacyjną. Tę ostatnią, w społeczeństwie postindustrialnym wykonują nie tylko urzędnicy, lecz nowa inteligencja. Prowadzi to do rozwoju zatrudniania w sferze usług i informacji, a w konsekwencji do powstania nowej mentalności społecznej. Por. D. Bell, *The Coming…*, s. 15–20 i 467 i n. Zob. także: A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problem bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 31–37. J. Sobczak, *Dylematy społeczeństwa informacyjnego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI wieku*, Elbląg 2006, s. 13–36; J. Sobczak, *Problemy społeczeństwa informacyjnego w dobie globalizacji*, T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007, s. 193–213; J. Sobczak, *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała,

internetowych[22]. Pojmowana była jako przestrzeń współpracy, niosąca za sobą zarówno pozytywne, jak i negatywne skutki. Do tych drugich zaliczano zwykle możliwości kontrolowania społeczeństwa za pomocą specjalnych narzędzi teleinformatycznych, stosowanych przez służby państwowe, co określano mianem cyberinwigilacji oraz możliwość wykorzystywania sieci przez przestępczość zorganizowaną (cyberprzestępczość), oraz do działań terrorystycznych (cyberterroryzm)[23]. Wskazuje się także, że cyberprzestrzeń jest obszarem, w którym możliwe jest prowadzenie działań wojennych (cyberwojna)[24].

Cyberprzestrzeń zdefiniował Departament Obrony Stanów Zjednoczonych, wskazując, że jest to „współzależna, powiązana ze sobą sieć infrastrukturalna technologii informacyjnej, obejmująca internet, sieci telekomunikacyjne, systemy komputerowe oraz systemy kierujące procesami produkcji i kontroli w sektorach strategicznych dla bezpieczeństwa narodowego"[25].

Pojęcie „cyberprzestrzeni" jest używane, jak wynika z powyższych rozważań, jako synonim „sieci", ale bywa, że odnosi się je także do telekomunikacji, jako fenomenu pozwalającego na łączenie się. „Widzialnym" są przewody, satelity, przekaźniki telekomunikacyjne, telewizory, telefony, komputery,

J. Iwanek (red.), *Demokratyzacja w dobie globalizacji*, t. 2, *Aspekty teoretyczne*, Katowice 2008, s. 52–79.

22 A. Nowak, *Cyberprzestrzeń…*, s. 7.

23 M. Pala, *Wybrane aspekty bezpieczeństwa w cyberprzestrzeni*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, nr 1(1), s. 115; S. Serwiak, *Cyberprzestrzeń jako źródło zagrożenia terroryzmem* [w:] E. Pływaczewski (red.), *Przestępczość zorganizowana, świadek koronny i terroryzm w ujęciu praktycznym*, Kraków 2005.

24 P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielniecki, K. Rajchel (red.), *Cyberterroryzm – nowe wyznawania XXI wieku*, Warszawa 2009, s. 46.

25 US Department of Defense Strategy for Operating in Cyberspace, Departament Obrony USA, lipiec 2011 r., cyt. za: A. Nowak, *Cyberprzestrzeń…*, s. 7. Godzi się zauważyć, że sformułowanie to bywa także tłumaczone w ten sposób, że cyberprzestrzeń to „globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnego (IT) oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery". Zob. J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego. Studia i Analizy" 2013, nr 9, s. 225–234. Wobec rozbieżności w tłumaczeniach należy przytoczyć definicję w angielskim oryginale *A global domain within the information environment consisting of the interdependent Network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

a „niewidzialnym" różne formy oprogramowania, przeglądarki, narzędzia do surfowania w sieci teleinformatycznej[26].

Pozostając w kręgu koncepcji amerykańskich trzeba zwrócić uwagę na definicję zawartą w Narodowej strategii dla bezpiecznej cyberprzestrzeni. W jej treści stwierdzono: „Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public, health, emergency services, government, defense, industrial base, information and telecommunications, energy, transportation,banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system —the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security"[27].

Sąd Najwyższy USA zdefiniował cyberprzestrzeń (cyberspace), jako „niekończącą się konwersację o światowym zasięgu". Wskazuje się przy tym, że cyberprzestrzeń jest miejscem nieograniczonej wymiany informacji, rozwoju życia społecznego, uczestniczenia w kulturze, utrzymywania różnego rodzaju więzi personalnych za pośrednictwem komputera[28].

W doktrynie, łącząc cyberprzestrzeń z licznymi przestępstwami, wskazuje się, że tożsamość w cyberprzestrzeni może przybrać trzy wymiary: tożsamości rzeczywistej, fikcyjnej i anonimowej. Wyróżnia się także tożsamość biurokratyczną i biograficzną, zaliczając do tej pierwszej dane przyporządkowane do

26 K.W. Grewlich, *„Cyberspace". Sector – specyfic. Regulatio and Competition Rules in European Telecommunications*, „Common Market Law Review" 1999, nr 6, s. 940.

27 Tekst strategii jest dostępny na stronie internetowej pod adresem: http://www.dhs.gov/national-strategy-secure-cyberspace. W tłumaczeniu polskim dokonanym przez J. Wasilewskiego definicja ta brzmi: „Nasza Krajowa infrastruktura krytyczna jest budowana przez publiczne, jak i prywatne instytucje funkcjonujące w sektorach rolnym, żywieniowym, zaopatrzenia w wodę, służby zdrowia, usług ratunkowych, rządowym, obronnym, przemysłowym, informacyjnym oraz telekomunikacyjnym, energetycznym, transportowym, bankowym oraz finansowym, chemicznym oraz materiałów niebezpiecznych, a także pocztowym oraz dostawczym. Cyberprzestrzeń stanowi ich układ nerwowy – system kontrolny naszego kraju. Cyberprzestrzeń jest zbudowana z setek tysięcy połączonych komputerów, serwerów, routerów, switchy oraz światłowodów, które umożliwiają pracę naszej infrastrukturze krytycznej. Stąd też zdrowe funkcjonowanie cyberprzestrzeni jest kluczowe dla naszej ekonomii oraz bezpieczeństwa narodowego". Zob. J. Wasilewski, *Zarys definicyjny…*, s. 228.

28 I. Matusiak, *Gra komputerowa jako przedmiot prawa autorskiego*, Warszawa 2013, passim.

określonej osoby w celu odróżnienia od innych i przybierające często postać numeru[29]. Żałować należy, że w obszarze naukowym tak rzadko zwraca się uwagę na te kwestie i dochodzi do przykrych sytuacji, kiedy później zaistniała na rynku wydawniczym, zajmująca się tą samą dziedziną działalności, co piszący wcześniej kolega, beztrosko funkcjonuje pod oczywiście swoim imieniem i nazwiskiem, nie zwracając uwagi na to, że jest to imię i nazwisko w literaturze występujące. Niekiedy zmusza to wcześniej publikującego badacza do tłumaczenia, że teksty, które pojawiają się tu i ówdzie nie są jego tekstami, a ten który później zaistniał na rynku w pełnej glorii, daje do zrozumienia, że rozmaite książki, artykuły to jego dzieła. Tymczasem wystarczyłoby w niektórych sytuacjach posłużyć się drugim imieniem, a w razie jego braku po prostu imię takie przybrać.

W literaturze zaproponowano definicję „cyberprzestrzeni globalnej" stwierdzając, że jest to system wymiany przetwarzania informacji (danych) funkcjonujących zgodnie z formalnymi zasadami i uregulowaniami prawnymi, obowiązującymi na terytorium poszczególnych państw działający dzięki połączeniu zasobów technicznych zlokalizowanych na terytorium każdego z nich. Cyberprzestrzeń RP proponuje się w doktrynie zdefiniować, jako system wymiany, przetwarzania informacji (danych) funkcjonujących zgodnie z formalnymi zasadami i uregulowaniami prawnymi, obowiązującymi na terytorium RP, działający dzięki połączeniu zasobów technicznych zlokalizowanych na jej terytorium[30].

29 S. Mason, *Validating identity for the electronic environment*, „Computer Law and Security Report" 2004, nr 3, s. 165; A. Sauer, *Online privacy and the online self*, „Privacy Law Bulletin" 2008, nr 9, s. 44; N. Archet [w:] *Identity Theft and Fraud*, Ottawa 2012, s. 22; B. De Vries, J. Tigchelaar, T. van der Linden, *Describing Identity Fraud: Towards a Common Definition*, „Scripted" 2008, nr 3, s. 485. Zob. także: A. Lach, *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015, s. 18–19. W odniesieniu do internetu i sieci teleinformatycznych wyróżnia się trzy rodzaje tożsamości: tożsamość osoby, tożsamość podmiotu kolektywnego oraz tożsamość sieciowa. Zob. A.M. Marschall, B.C. Tompset, *Identity theft in an online world*, „Computer Law and Security Report" 2005, nr 21, s. 129–130. Konstatuje się przy tym, że w sieci każda osoba może dysponować kilkoma tożsamościami, jedną rzeczywistą i kilkoma fikcyjnymi lub anonimowymi, wskazując, że w cyberprzestrzeni pojęcie tożsamości nabiera innego wymiaru, A. Lach, *Karnoprawna*..., s. 19.

30 A. Nowak, *Cyberprzestrzeń*..., s. 9.

System prawny Rady Europy wobec przestępstw w cyberprzestrzeni

Stopniowo pojęcie cyberprzestrzeni (ang. *cyberspace*) znalazło stałe obywatelstwo w języku potocznym[31] i zaczęło wdzierać się do języka prawniczego, a potem prawnego. W Konwencji Rady Europy o cyberprzestępczości z 23 listopada 2001 r.[32] nie użyto jednak terminu „cyberprzestrzeń". Natomiast w tytule Konwencji, w polskim tłumaczeniu, oraz w preambule i w art. 46 ust. 1 lit. b posłużono się określeniem „cyberprzestępczość", ale w art. 1 poświęconym definicjom, nie wyjaśniono jego treści[33]. Prace nad Konwencją Rady Europy o cyberprzestępczości były dość żmudne. Na pewnym etapie włączyła się w nie Rada Unii Europejskiej, wskazując, że powodem takiego kroku był przyjęty *Plan działania Unii Europejskiej w sprawie wspierania bezpiecznego wykorzystania sieci Internet*. We Wspólnym Stanowisku z dnia 27 maja 1999 r. zadeklarowano, że państwa członkowskie wspierać będą sporządzenie projektu Konwencji Rady Europy o cyberprzestępczości, wskazując, że przepisy Konwencji powinny odpowiednio uzupełnić prawo materialne i objąć przestępstwa przeciwko poufności, integralności oraz dostępności danych komputerowych, przestępstwa związane z komputerami, tak jak komputerowe oszustwo i fałszerstwo oraz przestępstwa związane z treścią, takie jak

31 M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2, s. 19–38. Zob. także: A. Tarkowski, *Internet jako technologia i wyobrażenie. Co robimy z technologią, co technologia robi z nami* [w:] D. Bartowski i inni, *Społeczna przestrzeń Internetu*, Warszawa 2006, s. 30–37.

32 Dz.U. z 2015 r., poz. 728. Konwencja ta została ratyfikowana przez Polskę dopiero 29 stycznia 2015 r., przy czym zgłoszono zastrzeżenia do art. 29 ust. 4 oraz deklaracje w odniesieniu do art. 24 ust. 7, art. 27 ust. 2 lit. a oraz art. 35 Konwencji. Por. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, passim.

33 Opiniujący Konwencję przed ratyfikacją M. Mróz zwracał jednak uwagę, że w językach oficjalnych Rady Europy istnieje pewna rozbieżność terminologii używanej w Konwencji. W tekście angielskim pojęcie „cyberprzestrzeni" nie występuje w ogóle, w tekście sporządzonym w języku francuskim dwukrotnie, przy czym raz w Preambule. W tłumaczeniu Konwencji na język niemiecki nie użyto, jak zauważył, w ogóle terminu „cyberprzestrzeń". Zob. M. Mróz, *Informacja nt. pojęcia cyberprzestrzeni oraz bezpieczeństwa i zagrożenia cyberprzestrzeni w prawie międzynarodowym i ustawodawstwie wybranych państw demokratycznych (w zw. z Drukiem sejmowym nr 4355)*, *Druk sejmowy nr 1757*, Warszawa, 22 lipca 2011. Zob. także: A. Szmyt, *Opinia prawna do przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Druk sejmowy nr 4355)*, Warszawa, dnia 11 lipca 2011 r.

pornografia dziecięca. Nie odniesiono się jednak w tym dokumencie do pojęcia cyberprzestrzeni[34].

Do innych poza Konwencją o cyberprzestępczości do inicjatyw Rady Europy w analizowanym obszarze wypada zaliczyć projekty: GLACY – Global Action against Cybercrime, Cybercrime@Octopus, organizację corocznych konferencji *Octopus Interface*, Partnerstwo Wschodnie – „Współpraca przeciwko Cyberprzestępczości" (*Eastern Partnership – Cooperation against Cybercrime – Project on Cybercime@EAPII*).

Godzi się jednak zauważyć, że Konwencję tę poprzedził raport *Przestępstwa związane z komputerem. Analiza polityki legislacyjnej*[35] Organizacji Współpracy Gospodarczej i Rozwoju (*Organization for Economic Co-operation and Development*) opublikowany w 1985 r. W jego treści znalazła się robocza definicja przestępstwa komputerowego rozumianego jako każde, bezprawne, nieetyczne i nieuprawnione zachowanie, którego przedmiotem jest automatyczne przetwarzanie lub transmisja danych. Ważne było także wyróżnienie pięciu kategorii zachowań godzących w funkcjonowanie sieci komputerowej. Wśród nich zaś: oszustwa komputerowego, fałszerstwa komputerowego, uszkodzenia danych komputerowych lub programów, naruszanie praw autorskich do programu komputerowego i nieuprawnione uzyskanie dostępu do komputera lub systemu telekomunikacyjnego w wyniku naruszenia zabezpieczeń[36].

Przeciwdziałanie przestępczości w cyberprzestrzeni w systemie prawa międzynarodowego uniwersalnego (powszechnego)

W systemie uniwersalnym powszechnym, czyli w systemie ONZ problemowi przestępczości poświęcono szereg rezolucji, z których najbardziej istotną wydaje się rezolucja nr 45/121 z dnia 14 grudnia 1990 r. dotycząca przestępstw związanych z wykorzystaniem komputerów. Pozostałe rezolucje dzieli się

34 Dz.Urz. UE L 1999, nr 142, s. 1.

35 *Computer – Related Crime. Analysis of legal Policy in the OECD Area, OECD, ICCP Series nr 10*, Paris 1986.

36 Szerzej w tym przedmiocie: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 152–156.

zwykle w myśl propozycji A.M. Hubbarda i S. Schjølberga[37] na trzy grupy, a mianowicie: rezolucje odnoszące się do rozwoju w dziedzinie informacji i telekomunikacji w kontekście rozwoju w dziedzinie informacji i bezpieczeństwa, rezolucje odnoszące się do walki z kryminalnymi nadużyciami technologii informatycznej oraz rezolucje odnoszące się do tworzenia światowej kultury cyberbezpieczeństwa, a także ochrony informatycznej infrastruktury krytycznej[38]. Poza tym szereg dokumentów dotyczących przeciwdziałania cyberprzestępczości wydało biuro ds. narkotyków i przestępczości, Międzynarodowy Związek Telekomunikacyjny, a także Grupa G7/G8[39]. Zwrócić także należy uwagę na Światowy Protokół dotyczący cyberbezpieczeństwa i cyberprzestępczości[40].

System prawa unijnego wobec zjawiska przestępczości w cyberprzestrzeni

Charakterystyczną cechą dla ustawodawstwa unijnego jest to, iż unika ona w miarę konsekwentnie pojęcia „cyberprzestrzeni", zastępując ją określeniem „systemy informatyczne". Przykładem może być dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady nr 2005/222/WSiSW[41]. W części wstępnej wspomnianej dyrektywy zwrócono uwagę, że „systemy informatyczne (sic! przyp. mój J.S.) stanowią podstawowy element relacji politycznych, społecznych i gospodarczych w Unii". Wskazano, że „zależność społeczeństwa od tego typu systemu jest bardzo wysoka i stale rośnie. Dobre funkcjonowanie i bezpieczeństwo tych systemów Unii są niezbędne dla rozwoju rynku wewnętrznego oraz konkurencyjnej i innowacyjnej gospodarki. Podkreślono także, ze zarówno w obszarze Unii, jak i globalnie rośnie zagrożenie atakami na systemy informatyczne, a zwłaszcza atakami dokonywanymi

37 A.M. Hubbard, S. Schjølberg, *Harmonizing national legal approaches on cybercrime*, s. 6, https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

38 Omówienie wspomnianych rezolucji zob. F. Radoniewicz, *Odpowiedzialność karna…*, s. 196–200.

39 Prezentacja tych dokumentów zob. F. Radoniewicz, *Odpowiedzialność karna…*, s. 200–217.

40 S. Ghernaouti-Helie, S. Schjølberg, *Global Treaty on Cybersecurity and Cyber Crime, Second edition 2011*, https://www.researchgate.net/publication/236200268_A_global_treaty_on_cybersecurity_and_cybercrime.

41 Dz.Urz. UE L 2013, nr 218, s. 8.

w ramach przestępczości zorganizowanej". Warto zauważyć, że w tekście tym nie użyto w ogóle pojęcia „cyberprzestrzeni". Pojęcie to pojawiło się natomiast w rezolucji Parlamentu Europejskiego z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony (2012/2096(INI)) pkt 35, w którym stwierdzono, że ochrona krytycznej infrastruktury teleinformatycznej uwzględniona jest w strategii bezpieczeństwa wewnętrznego UE w kontekście zwiększenia poziomu bezpieczeństwa obywateli i przedsiębiorstw w cyberprzestrzeni[42].

W prawie Unii Europejskiej od dość dawna funkcjonowały akty normatywne o charakterze niewiążącym, których zadaniem jest ochrona bezpieczeństwa systemów informatycznych. Zaliczyć do nich należy decyzję ramową Rady 2005/222/WSiSW z 24 lutego 2005 r.[43] Nie wolno także zapominać o treści rozporządzenia 2004/460/WE Parlamentu Europejskiego i Rady z 10 marca 2004 r. ustanawiającego Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[44]. Z opublikowanego przez Komisję Europejską w dniu 14 lipca 2008 r. sprawozdania z wykonania decyzji ramowej 2005/222/WSiSW wynika, że większość państw członkowskich podjęła kroki w celu implementacji postanowień decyzji ramowej. Niemniej wydając dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z dnia 20 sierpnia 2013 r. dotyczącej ataków na systemy informacyjne, zdecydowano się zastąpić tą dyrektywą decyzję ramową Rady 2005/222/WSiSW[45]. W treści dyrektywy sformułowano szereg przestępstw polegających m.in. na: niezgodnym z prawem dostępie do systemów informatycznych (art. 3), niezgodną z prawem ingerencją w systemie informatycznym

42 Dz.Urz. UE C 2015, nr 419, s. 145. W dalszej części tego dokumentu w pkt 44 odniesiono się do konieczności szerszej międzynarodowej współpracy i ostatecznego porozumienia dotyczącego ustalenia wspólnego rozumienia norm zachowania w cyberprzestrzeni. W pkt 55 stwierdzono, że UE i USA to największe źródła cyberprzestrzeni (sic!) i jej użytkowników.

43 Dz.Urz. UE L 2005, nr 69, s. 67. Od razu wypada zwrócić uwagę na istniejące rozbieżności między wspomnianą decyzją ramową a przytoczoną wyżej Konwencją o cyberprzestępczości w systemie Rady Europy. W uzasadnieniu decyzji ramowej odwołano się do wytycznych z zalecenia OEDC C (92) 188 z 26 listopada 1992 r. dotyczącego wytycznych w zakresie bezpieczeństwa systemów informatycznych (92) 188. *Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C (92) 188/ FINAL]*. Wspomniane zalecenie (92) zostało zastąpione przez zalecenie OECD C (2002) 131 z 25 lipca 2002 r. w sprawie wytycznych w zakresie bezpieczeństwa systemów i sieci informatycznych w kierunku kultury bezpieczeństwa. *Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security of 25 July 2002 [C (2002) 131]*. Wytyczne te zostały zrewidowane po raz pierwszy w 2007 r. W grudniu 2013 r. zakończono kolejną ich rewizję.

44 Dz.Urz. UE L 2004, nr 77, s. 1.

45 Dz.Urz. UE L 2013, nr 218, s. 8.

(art. 4), niezgodną z prawem przechwytywania środkami technicznymi niepublicznych przekazów internetowych (art. 6) oraz na bezprawnym wytwarzaniu, sprzedaży, dostarczaniu w celu użycia, przewozie i posiadaniu narzędzi do popełniania przestępstw komputerowych (art. 7). Przewidziano także karalność podżegania, pomocnictwa do wszystkich przestępstw przewidzianych w dyrektywie oraz usiłowanie popełnienia przestępstw polegających na bezprawnej ingerencji w system informatyczny oraz ingerencji w dane komputerowe w systemie informatycznym[46].

Dla podjętej w tym miejscu problematyki, istotniejsze znaczenie wydaje się mieć dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze o łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[47]. Dyrektywa ta generalnie zakazuje przejmowania kontroli nad komputerami, przechwytywania komunikatów przesłanych za pośrednictwem publicznych sieci komunikacyjnych, nakazując jednocześnie państwom członkowskim zapewnienie poufności komunikacji i nie pozwalając na monitorowanie, nagrywanie, przechowywanie, kontrolowanie komunikatów i związanych z nimi danych o ruchu przez osoby inne niż użytkownicy bez zgody zainteresowanych użytkowników. Wyjątkiem jest działanie w celu zapewnienia bezpieczeństwa narodowego i bezpieczeństwa państwa, obron-

46 W opinii *Electronic Frontier Foundation (EFF)* wskazano, że istnieje możliwość pociągnięcia do odpowiedzialności karnej aktywnych użytkowników p2p tj. np. Tor, która daje możliwość zapewnienia sobie anonimowości w trakcie korzystania z internetu lecz nie ma na celu zapewnienia anonimowości w związku z wymianą plików, jak to ma miejsce, w takich systemach jak ANts, P2P, Freenet, GNUnet czy MUTE. Z założenia Tor służyć ma obronie przed wszystkimi sieciowej inwigilacji, umożliwiając swobodną, wolną od kontroli państwa wymianę informacji. Zob. *EFF Comments on the Draft Directive on Attacks against Computer Systems*, https://www.eff.org/Directive-Attacks-against-Computer-Systems. Jak wskazuje F. Radoniewicz podniesiony w opinii problem nie dotyczy polskiego systemu prawnego z uwagi na to, że przewiduje on możliwość podżegania i pomocnictwa w odniesieniu do konkretnych osób, a nie do niesprecyzowanej, nieokreślonej grupy podmiotów. F. Radoniewicz, *Odpowiedzialność karna…*, Warszawa 2016, s. 198.

47 Dz.Urz. UE L 2002, nr 201, s. 37, zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE Dz.Urz. UE L 2009, nr 337, s. 11. Zob. w tej kwestii: M.B. Kanarski, J. Radzikowska, *Nowe ramy regulacyjne dla usług łączności elektronicznej* [w:] M. Rogalski (red.), *Prawo telekomunikacyjne*, LEX 2011. Z problematyką tą wiąże się także dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) Dz.Urz. UE L 2002, nr 108, s. 33, zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/140/WE z 25 listopada 2009 Dz.Urz. UE L 2009, nr 337, s. 37 i sprostowana Dz.Urz. UE L 2013, nr 241, s. 8.

ności, bezpieczeństwa publicznego oraz dążenie do zapobiegania, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej[48].

Naruszeniem prywatności jest w wielu przypadkach posługiwanie się mową nienawiści mimo istnienia międzynarodowych standardów zakazujących tego rodzaju działań. Wskazać wśród nich należy w pierwszym rzędzie decyzję ramową z dnia 28 listopada 2008 r. 2008/913/WSiSW w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych[49]. W treści art. 1 decyzji ramowej nałożono na każde państwo członkowskie Unii Europejskiej zastosowanie niezbędnych środków w celu zapewnienia karalności czynów polegających na publiczne nawoływanie do przemocy lub nienawiści skierowanej przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, popełnianych także przez publiczne rozpowszechnianie lub rozprowadzanie tekstów, obrazów lub innych materiałów (art. 1 ust. 1 pkt a i b). Ponadto w decyzji ramowej wskazano, że każde państwo członkowskie Unii Europejskiej ma zapewnić karalność czynów polegających na publicznym aprobowaniu, negowaniu lub rażącym pomniejszaniu zbrodni ludobójstwa, zbrodni przeciwko ludzkości oraz zbrodni wojennych w rozumieniu art. 6, 7 i 8 statutu Międzynarodowego Trybunału Karnego skierowanych przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko tej grupie lub jej członkowi (art. 1 ust. 1 pkt c). Zobowiązano w końcu państwa do zapewnienia karalności czynów polegających na publicznym aprobowaniu, negowaniu lub rażącym pomniejszaniu zbrodni określonych w art. 6 Karty Międzynarodowego Trybunału Wojskowego załączonej do porozumie-

48 E. Preis, *Glosa do wyroku Trybunału Sprawiedliwości z dnia 29 stycznia 2008, C – 275/06*, „Europejski Przegląd Sądowy" 2009, nr 4, s. 49.

49 Dz.Urz. UE 2008 L 328/55 z 6 grudnia 2008 r. Decyzja ta rozszerza treść zawartą we Wspólnym Działaniu Rady 96/443/WSiSW z dnia 15 lipca 1996 r. dotyczącą działania w celu zwalczania rasizmu i ksenofobii (Dz.Urz. UE 1996 L 185 z 24 lipca 1996 r.), deklarując istnienie konieczności dodatkowych działań legislacyjnych w związku z potrzebą dalszego zbliżenia przepisów ustawowych i wykonawczych państw członkowskich oraz pokonania przeszkód w skutecznej współpracy sądowej, wynikających głównie z rozbieżności w systemach prawnych poszczególnych państw członkowskich, przy czym w treści art. 11 decyzji ramowej uchylono Wspólne Działanie 96/443/WSiSW.

nia londyńskiego z dnia 8 sierpnia 1945 r., a skierowanych przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko tej grupie lub jej członkowi (art. 1 ust. 1 pkt d).

Niezwykle istotna w prawie unijnym jest dyrektywa Parlamentu Europejskiego i Rady (UE) 2017 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW[50]. W jej treści przypomniano przyjęty przez Radę Europy w 2015 r. Protokół Dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim i ksenofobicznym popełnionych przy użyciu systemów komputerowych[51]. Warto zauważyć, że w treści tego Protokołu – ratyfikowanego przez Polskę 29 stycznia 2015 r., zdefiniowano „materiały rasistowskie i ksenofobiczne", wskazując, że pod tym terminem należy rozumieć każdy materiał pisemny, każdy wizerunek lub każde inne wyrażenie myśli i teorii, które nawołują, popierają lub podżegają do nienawiści, dyskryminacji lub przemocy przeciw jakiejkolwiek osoby lub grupie osób ze względu na rasę, kolor, pochodzenie narodowe lub etniczne, jak również religię, jeżeli wykorzystywana jest ona jako pretekst do zachowań o charakterze rasistowskim lub ksenofobicznym, gwałcących prawa człowieka i stanowiących zagrożenie dla rządów prawa i demokratycznej stabilności. W treści Protokołu zwrócono uwagę na środki, jakie państwa unijne powinny podjąć na szczeblu krajowym w kwestii zwalczania: rozpowszechniania materiałów rasistowskich i ksenofobicznych w systemie komputerowym; gróźb i zniewag spowodowanych rasizmem i ksenofobią; a także w kwestii zwalczania, zaprzeczania lub poważnego umniejszania znaczenia, akceptacji lub usprawiedliwienia, zbrodni ludobójstwa oraz zbrodni przeciwko ludzkości.

We wspomnianej dyrektywie z 15 marca 2017 r. zauważono także, że przestępstwo związane z publicznym nawoływaniem do popełniania czynów mający charakter terrorystyczny obejmuje m.in. pochwalanie i usprawiedliwianie terroryzmu, rozpowszechnianie w internecie lub poza nim wiadomości lub obrazów, w tym obrazów dotyczących ofiar terroryzmu, w celu zdobycia poparcia dla idei terrorystycznych lub w celu poważnego zastraszania ludności.

50 Dz.Urz. UE L 2017, nr 88, s. 6.
51 Dz.U. 2015, poz. 730.

Taki czyn – jak wskazano – powinien podlegać karze, jeżeli stwarza niebezpieczeństwo popełnienia aktów terrorystycznych. W każdym konkretnym przypadku przy ocenianiu, czy takie niebezpieczeństwo istnieje, uwzględnić należy szczególne okoliczności sprawy, takie jak autora i adresata wiadomości, a także kontekst, w jakim doszło do popełnienia czynu. To czy niebezpieczeństwo jest istotne, i czy ma ono wiarygodny charakter, należy również brać pod uwagę przy stosowaniu przepisu o publicznym nawoływaniu zgodnie z prawem krajowym.

Podkreślono także, że dyrektywa zawiera wyczerpujący wykaz poważnych przestępstw, takich jak ataki na życie ludzkie stanowiących czyny umyślne, które można zakwalifikować jako przestępstwa terrorystyczne wyłącznie w przypadku, gdy zostały popełnione w określonym celu terrorystycznym, mianowicie, aby poważnie zastraszyć ludność, bezprawnie zmusić rząd lub organizację międzynarodową do podjęcia lub zaniechania działania, lub aby poważnie zdestabilizować lub zniszczyć podstawowe struktury polityczne, konstytucyjne, gospodarcze lub społeczne danego państwa lub danej organizacji międzynarodowej. Groźby popełnienia takich czynów umyślnych również – jak podkreślono w motywach dyrektywy – należy uznawać za przestępstwa terrorystyczne, jeżeli obiektywne przesłanki wskazują, że dopuszczono się ich, kierując się jednym z wymienionych celów terrorystycznych. Natomiast czynów, których celem jest na przykład zmuszenie rządu do podjęcia lub zaniechania jakiegokolwiek działania, ale których nie umieszczono w wyczerpującym wykazie poważnych przestępstw, nie uznaje się zgodnie z niniejszą dyrektywą za przestępstwa terrorystyczne.

Zauważono także, że niezbędne jest uznanie za przestępstwo podróży zagranicznych w celach terrorystycznych, obejmując nie tylko popełnianie przestępstw terrorystycznych i prowadzenie lub odbywanie szkolenia, lecz także uczestnictwo działalności grupy terrorystycznej. Podkreślono, że karze powinno w państwach członkowskich podlegać – jako pomocnictwo w terroryzmie lub finansowanie terroryzmu – udzielanie materialnego wsparcia terroryzmowi poprzez osoby zajmujące się dostarczaniem lub przemieszczaniem usług, mienia i towarów, w tym transakcji handlowych obejmujących wprowadzanie na obszar Unii lub wyprowadzanie z tego obszaru, takich jak sprzedaż, nabycie lub wymiana dóbr kultury o wartości archeologicznej, artystycznej, historycznej lub naukowej, które nielegalnie wywieziono z obszaru kontrolowanego przez grupę terrorystyczną w momencie wywozu lub osoby będące pośrednikami w takich działaniach, jeżeli dokonywane są one ze świadomością, że operacje te lub pochodzące z nich przychody są w całości lub w części

przeznaczone do celów terrorystycznych lub przysporzą one korzyści grupom terrorystycznym. Podniesiono, że państwa członkowskie powinny zapewnić środki ochrony wsparcia i pomocy ofiarom terroryzmu zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2012/29/UE z dnia 25 października 2012 r. ustanawiającą normy minimalne w zakresie praw, wsparcia i ochrony ofiar przestępstw oraz zastępującą decyzję ramową Rady 2001/220/WSiSW[52]. W treści dyrektywy wskazano czyny umyślne, które zgodnie z prawem krajowym ze względu na swój charakter lub kontekst mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej i z tego tytułu powinny być zaliczone do przestępstw terrorystycznych. Wskazano wśród nich m.in. także niezgodne z prawem ingerencje w systemy informatyczne, utrudnianie lub zakłócanie ich funkcjonowania, przekazanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych[53].

W doktrynie podkreśla się, że standardy w zakresie przestępczości w cyberprzestrzeni, w tym także ścigania mowy nienawiści wypracowują także judykaty Europejskiego Trybunału Praw Człowieka, Komitetu Praw Człowieka ONZ, Rady Europy oraz w przyszłości Trybunału Sprawiedliwości w Luksemburgu[54]. Można poddawać w wątpliwość możliwość zwalczania mowy

52 Dz.Urz. UE L 2012, nr 315, s. 57. Zob. E. Bieńkowska, L. Mazowiecka (red.), *Dyrektywa Parlamentu Europejskiego i Rady ustanawiająca normy minimalne w zakresie praw wsparcia i ochrony ofiar przestępstw. Komentarz*, Warszawa 2014, passim.

53 Oprócz tego zaliczono do czynów terrorystycznych działania, których celem jest poważne zastraszenie ludności, bezprawne zmuszenie rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania, poważna destabilizacja lub zniszczenie podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych jakiegoś państwa lub organizacji międzynarodowej, przejawiająca się w atakach na życie ludzkie, które mogą spowodować śmierć, w atakach na integralność fizyczną osoby, a także: porwanie lub branie zakładników; powodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury w tym także systemu informacyjnego, platform na szelfie kontynentalnym, miejsc publicznych, mienia prywatnego – jeżeli zniszczenia te mogą zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze. Ponadto za przestępstwa terrorystyczne uznano wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie, lub używanie materiałów wybuchowych lub broni, w tym także chemicznej, biologicznej, radiologicznej lub jądrowej, a także badania nad taką bronią; uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi, względnie wybuchów zagrażających życiu ludzkiemu, wreszcie zakłócanie lub przerywanie dostaw wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, czego rezultatem jest zagrożenie życia ludzkiego.

54 A. Gliszczyńska-Grabias, *Międzynarodowoprawne standardy wolności a mowa nienawiści* [w:] D. Bychawska-Sinarska, D. Głowacka (red.), *Mowa nienawiści w internecie: jak z nią walczyć?*, Warszawa 2013, s. 45–50.

nienawiści środkami prawa karnego[55], aczkolwiek istnieje wyraźna tendencja do tego, aby przepisy prawa karnego użyć do tego właśnie celu[56].

Wypada przy tym zauważyć, że ilość regulacji normatywnych nie przekłada się na sukcesy w zwalczaniu zjawiska przestępczości i programy oraz działania Rady Europy i Unii Europejskiej zmierzające w kierunku ochrony użytkowników internetu, dają nikłe rezultaty[57]. Niewiele więcej przynoszą inicjatywy obywatelskie, działania lobbingowe, a także próby społecznych re-

55 Czyni tak Ewa Łętowska, stwierdzając, że: „Granice między słowem, bez którego nie ma demokracji, i słowem, które zabija wolność lub prawo innego człowieka, obecnie nie rysują się u nas jasno. Sądowy standard, który służy ich wytyczeniu na tle prawa, znajduje się ciągle na etapie ustalania metodą prób i błędów". Zwraca ona jednak uwagę, że istnieje „wielka różnica między celowym zniesławieniem, obrażaniem, szczuciem, a krytycznym dyskursem publicznym. Wolność słowa i wolność wyrażania poglądów nie usprawiedliwia naruszania praw i wolność innych. To elementarz praw człowieka". Dodaje przy tym, „dlatego nie przekonują mnie ci, którzy uważają, że w internecie i właśnie akurat w nim, tylko dlatego, że jest internetem można umieścić wszystko o wszystkim. W internecie wolno tyle i tylko tyle, ile wolno w innych mediach. »Złe słowo« to słowo szczujące, raniące, poniżające, szydzące, nawołujące do czynów gwałtownych". E. Łętowska, *Zwodnicze pokusy karania hate speech* [w:] D. Bychawska-Siniarska, D. Głowacka (red.), *Mowa nienawiści w internecie: jak z nią walczyć?*, Warszawa 2013, s. 18–19. Zob. także: A. Śledzińska-Simon, *Decyzja ramowa w sprawie zwalczania pewnych form przejawów rasizmu i ksenofobii jako trudny kompromis wobec mowy nienawiści w Unii Europejskiej* [w:] R. Wieruszewski, M. Wyszykowski, A. Bodnar, A. Gliszczyńska-Grabias (red.), *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010, s. 93–113.

56 Por. w tym przedmiocie I. Hare, J. Weinstein (red.), *Extreme Speech and Democracy*, Oxford 2009; A. Cortese, *Opposing hate speech*, Westport 2006; R. Cohen-Almagor, *Holocaust Denial is a Form of Hate Speech*, „The Amsterdam Law Forum" 2009, no. 2; D.O. Brink, *Millian Principles, Freedom of Speech, and Hate Speech*, „Legal Theory" 2001, no. 7; N. Ghanea, *Expression and Hate Speech in the ICCPR: Compatible or Clashing?*, „Religion and Human Rights" 2010, no. 5.

57 Zob. m.in. *Program Safer Internet Action Plan* ustanowiony *Decyzją Parlamentu Europejskiego i Rady nr 276/1999/WE z dnia 25 stycznia 1999 r. przyjmującą wieloletni plan działań Wspólnoty w zakresie promowania bezpieczniejszego korzystania z Internetu poprzez zwalczanie sprzecznych z prawem i szkodliwych treści w światowych sieciach komputerowych* Dz.Urz. UE L, 1999, L 33 z 6 luty 1999 r. zmieniona Decyzją Parlamentu Europejskiego i Rady nr 1151/2003/WE z 16 czerwca 2003, Dz.Urz. UE L 162 z 1 lipca 2003. Program *Safer Internet Plus* (2005–2008) przyjęty Decyzją Parlamentu Europejskiego i Rady nr 854/2005/WE z 11 maja 2005 r. w sprawie ustanowienia wieloletniego programu wspólnotowego na rzecz promowania bezpieczniejszego korzystania z internetu i nowych technologii sieciowych Dz.Urz. UE L 2005, nr 149, s. 1. Obowiązywanie tej decyzji wygasło z dniem 31 grudnia 2008 r. Program *Safer Internet* wynikający z decyzji Parlamentu Europejskiego i Rady nr 1351/2008/WE z 16 grudnia 2008 r. w sprawie ustanowienia wieloletniego, wspólnotowego programu ochrony dzieci korzystających z internetu oraz z innych technologii informacyjnych Dz.Urz. UE L 2008, nr 348, s. 118. Kolejnym projektem jest *Roundtable* prowadzony w ramach programu *Safer Internet Action Plan*. Zob. *Youth Protection Roundtable*, www.yprt.ue.

gulacji[58]. W tej sytuacji wydaje się być uzasadnione stanowisko wyrażone jakiś czas temu w literaturze, iż internet jawi się jako przysłowiowa „butelka", z której nieostrożnie wypuszczono złośliwego dżina, który nie bacząc na nic narusza prywatność, depcze godność i cześć terroryzując swoimi działaniami przerażone społeczności. Za tym dżinem kryją się jednak złośliwi i przebiegli lub jedynie obojętni na cudzą krzywdę ludzie[59].

Zwalczenie cyberprzestępczości w polskim systemie prawnym

W polskim systemie prawnym definicja cyberprzestrzeni pojawiła się w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[60], po nowelizacji tej ustawy ustawą z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polski oraz niektórych innych ustaw[61]. W myśl art. 2 ust. 1b dodanym przez art. 1 pkt 2 wspomnianej ustawy z 30 sierpnia 2011 r. przez cyberprzestrzeń należy rozumieć przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[62] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Identyczne rozwiązanie wprowadzono: do tekstu ustawy z 21 czerwca 2002 r. o stanie wyjątkowym – przez art. 2 ust. 1a w oparciu o art. 2 pkt 2 ustawy z 30 sierpnia 2011 r.[63] o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw oraz do tekstu ustawy z 18 kwietnia 2002 r. o stanie

58 M. Gruchoła, *Ochrona użytkowników Internetu w państwach Unii Europejskiej*, Lublin 2012, s. 267–302.
59 J. Sobczak, K. Kakareko, *Odpowiedzialność za przestępstwa popełnione w sieci, a kwestia prywatności* [w:] J. Sobczak, K. Chałubińska-Jentkiewicz, K. Kakareko, *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, s. 1–32.
60 T.j. Dz.U. 2016, poz. 851.
61 Dz.U. 2011, nr 222, poz. 1323.
62 Dz.U. 2005, nr 64, poz. 565 ze zm.
63 Dz.U. 2011, nr 222, poz. 1323.

klęski żywiołowej[64], dodając art. 3 ust. 1 pkt 4 przez art. 3 pkt 1 wspomnianej już ustawy z 30 sierpnia 2011 r.[65]

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczpospolitej Polskiej 2022 przyjęta 9 kwietnia 2013 r. uchwałą nr 67 Rady Ministrów[66] nie definiuje pojęcia „cyberprzestrzeni", natomiast terminem tym się posługuje, wskazując, że do głównych działań pogłębienia współpracy na rzecz bezpieczeństwa cybernetycznego na forum NATO i UE należy uwzględnienie w polityce bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej nowych elementów wynikających z prac NATO i UE nad polityką bezpieczeństwa cybernetycznego. Wskazano także, że dążąc do nasycenia nowoczesnym uzbrojeniem i sprzętem wojskowym sił zbrojnych, trzeba doprowadzić do tego, aby były one odporne na zagrożenia z cyberprzestrzeni. Za główne działania w zakresie podwyższania stopnia zabezpieczeń zasobów teleinformatycznych administracji publicznych i państwowej przed zagrożeniami sieci internet oraz terroryzmem, uznano przyjęcie polityki ochrony cyberprzestrzeni Rzeczpospolitej Polskiej[67]. Skonstatowano przy tym, że wzrost zagrożeń w obszarze cyberprzestrzeni wymaga dostosowywania i ciągłego rozwijania istniejących struktur systemu reagowania, wiążąc to z rozwojem Rządowego Zespołu Reagowania na Incydenty Komputerowe. Wskazano, że posiadania przez Agencję Bezpieczeństwa Wewnętrznego oraz resort obrony narodowej silnych wyposażonych w zaawansowane technologie zespołów reagowania, usprawni realizowanie współpracy międzynarodowej oraz pozwoli osiągnąć nowe zdolności operacyjne w zakresie zadań reagowania na incydenty bezpieczeństwa teleinformatycznego oraz dowodzenia i kierowania w celach przestrzeni. Nałożono przy tym na ministra właściwego do spraw administracji publicznej, informatyzacji i łączności zadanie opracowanie polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. Podkreślając, że projekt taki winien zostać przyjęty przez Radę Ministrów jeszcze w 2013 r.

64 T.j. Dz.U. 2014, poz. 333 ze zm.

65 Zob. w tym przedmiocie J. Kosiński, *Cyberprzestępczość* [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013, s. 462–463. F. Radoniewicz, *Odpowiedzialność karna…*, s. 67.

66 M.P. 2013, poz. 377.

67 Odwołano się w tym miejscu do dokumentu przyjętego przez Komitet Rady Ministrów ds. Cyfryzacji w dniu 28 listopada 2012 r.

Uchwałą nr 252 Rady Ministrów z 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na 2015–2019”[68], precyzując założenia i systematykę programu, podkreślono, że winien być on skorelowany z Polityką Ochrony Cyberprzestrzeni. Zauważono także, że cyberprzestrzeń może być istotną sferą działalności terrorystycznej, wykorzystywaną przez organizacje terrorystyczne, zarówno do prowadzenia bezpośrednich ataków na serwery rządowe w celu uniemożliwienia ich funkcjonowania, dezinformacji lub pozyskiwania danych, jak i upowszechniania radykalnej ideologii, pozyskiwania ich zwolenników, czy prowadzenia instruktażu w zakresie podejmowania indywidualnych aktów terroru. Może być ona także – jak zauważono – wykorzystywana do dokonywania nielegalnego transferu środków finansowych na działalność terrorystyczną. Zdefiniowano, że atak cyberterrorystyczny winien być rozumiany, jako nielegalne działanie w cyberprzestrzeni o podłożu politycznym lub ideologicznym ukierunkowane na wywołanie strachu i skutkujące przemocą przeciwko ludziom lub mieniu, którego celem jest wymuszanie na rządzie oraz społeczeństwie realizacji celów politycznych lub społecznych zakładanych przez atakującego. Atakami terrorystycznymi mogą być więc – jak stwierdzono – nielegalne groźby i ataki przeciwko komputerom, sieciom komputerowym i informacjom w nich przechowywanym, a także działania sabotażowe prowadzone w cyberprzestrzeni, w tym także w odniesieniu do infrastruktury krytycznej oraz prowadzenie dezinformacji. Wskazano, że na poziomie strategicznym Rada Ministrów może podjąć uchwałę o skierowaniu do prezydenta wniosku o wprowadzenie stanu wyjątkowego w razie zewnętrznego zagrożenia państwa spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni i wnioskować o wprowadzenie stanu wojennego. Wywiedziono, że należy intensyfikować działania właściwych służb i instytucji w zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni. Dążąc do ochrony w cyberprzestrzeni wskazano na konieczność jej monitorowania i zwalczania zagrożeń, i ataków o charakterze cyberterrorystycznym[69]. W dalszej części Narodowego Programu Antyterrorystycznego w sposób szczegółowy w załącznikach wskazano na konieczność współdzia-

68 M.P. 2014, poz. 1218.

69 Kwestią przeciwdziałania zagrożeniom w cyberprzestrzeni poświęcony jest dokument *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* przyjęty uchwałą nr 111/2013 Rady Ministrów z 25 czerwca 2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html.

łania z organizacjami międzynarodowymi zajmującymi się przeciwdziałaniem i zwalczaniem zagrożeń o charakterze terrorystycznym, w tym z Organizacją Narodów Zjednoczonych, Unią Europejską, NATO, Radą Europy, OBWE. Zauważyć jednak należy, że posługując się wielokrotnie terminem „cyberprzestrzeń" w żadnym miejscu wspomnianego dokumentu nie zdefiniowano tego pojęcia[70].

W uchwale nr 23 Rady Ministrów z 8 marca 2016 r. w sprawie „Programu ograniczenia przestępczości i aspołecznych zachowań *Razem Bezpieczniej im. Władysława Stasiaka na lata 2016 i 2017*"[71] wskazano formułując jako jeden z celów szczegółowych, iż edukacja dla bezpieczeństwa powinna dotyczyć także cyberprzestrzeni. Potrzeba współpracy w zakresie zapobiegania i wykrywania sprawców przestępstw pojawiła się także w umowach 2 lipca 2005 r. między Rządem Rzeczypospolitej Polskiej a Rządem Indonezji o współpracy w zwalczaniu międzynarodowej przestępczości zorganizowanej i innych rodzajów przestępczości[72] oraz w umowie z dnia 9 października 2006 r. między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnej Republiki Brazylii o współpracę w zakresie zwalczania przestępczości zorganizowanej i innych rodzajów przestępczości[73].

Pojęcie cyberprzestrzeni zdefiniowano jednak we wspomnianym już dokumencie *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* z 25 czerwca 2013 r.[74] Cyberprzestrzeń zdefiniowano: „jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności

70 Należy podkreślić, że ustawą z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz.U. 2015, poz. 2281 ze zm.) w art. 1 pkt 1 wskazano, że dział informatyzacja obejmuje także bezpieczeństwo cyberprzestrzeni – jednak i tu z oczywistych względów nie zdefiniowano pojęcia cyberprzestrzeń.

71 M.P. 2016, poz. 293

72 Dz.U. 2016, poz. 1660.

73 Dz.U. 2016, poz. 1323.

74 http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html. Został on opracowany w Ministerstwie Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego w oparciu o: omówiony 9 marca 2009 r. przez Komitet Stały Rady Ministrów dokument „Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia", okresowe raporty o stanie bezpieczeństwa obszaru gov.pl, publikowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, decyzję przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji nr 1/2012 z dnia 24 stycznia 2012 r. w przedmiocie powołania Zespołu zadaniowego do spraw ochrony portali rządowych.

podmiotów realizujących zadania publiczne[75] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami; zgodnie z art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[76], art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym[77] oraz art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej"[78]. Natomiast cyberprzestrzeń Rzeczypospolitej Polskiej określono jako: „cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)". Wypada zauważyć, że w oparciu o te rozwiązania cyberprzestrzeń nie będzie obejmowała komputerów, ponieważ wskazuje na tzw. „urządzenia końcowe", czyli modem, telefon, router, ewentualnie karta sieciowa, które są „zakończeniem sieciowym", wskazanych w przytoczonej definicji w przepisach prawa. W literaturze podkreśla się, że należałoby zmienić definicję cyberprzestrzeni i cyberprzestrzeni RP w taki sposób, aby ta definicja obejmowała zasoby techniczne każdego użytkownika zarówno osoby fizycznej, obywatela oraz przedsiębiorcy. Zwraca się także uwagę, że używane w dokumencie pojęcie „cyberatak" nie obejmuje swoim zakresem ataków przeprowadzonych z cyberprzestrzeni RP na cyberprzestrzeń innych państw. Ma być to wynikiem tego, że pojęciem cyberprzestrzeni zostało zawężone do zasobów technicznych opisanych w przepisach prawa polskiego, tj. w pierwszym rzędzie do ustawy z dnia 17 maja 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz do prawa telekomunikacyjnego[79]. Z faktu, że pojęcie „cyberprzestrzeń" użyte w tym dokumencie nie obejmuje swoim zakresem pojęciowym w cyberprzestrzeni innego państwa, ewentualnie w cyberprzestrzeni globalnej, można by wysnuć wniosek, że atak przeprowadzony z wykorzystywaniem cyberprzestrzeni RP w odniesieniu do cyberprzestrzeni innego państwa nie jest cyberatakiem.

Przestępstwa popełniane przy użyciu komputerów nie mają charakteru jednorodnego. Wyróżnia się wśród nich skierowane przeciwko ochronie

75 Dz.U. nr 64, poz. 565 ze zm.
76 Dz.U. nr 156, poz. 1301 ze zm.
77 Dz.U. nr 113, poz. 985 ze zm.
78 Dz.U. nr 62, poz. 558 ze zm.
79 A. Nowak, *Cyberprzestrzeń*..., s. 9.

informacji, zawarte w rozdz. XXXIII k.k.[80], przestępstwa przeciwko mieniu[81] i wiarygodności dokumentów[82], do innych przestępstw komputerowych zwykło się zaliczać sprowadzanie powszechnego niebezpieczeństwa na skutek zakłócenia procesów automatycznego przetwarzania danych (art. 165 § 1 pkt 4 k.k.), szpiegostwo komputerowe (art. 130 § 3 k.k.), rozpowszechnianie oraz posiadanie treści pornograficznych przedstawiających małoletniego lub uzyskanie do nich dostępu (art. 202 § 4 a, b i c k.k.), nawiązywanie kontaktu z małoletnim w celu produkowania lub utrwalania treści pornograficznych za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej (art. 200 a k.k.).

Oczywiście przy użyciu komputera za pośrednictwem internetu, możliwe jest także propagowanie faszyzmu lub innego totalitarnego ustroju państwa (art. 256 k.k.), znieważanie grup ludności lub poszczególnych osób z powodu ich przynależności narodowej, etnicznej i rasowej, wyznaniowej (art. 257 k.k.), ujawnianie tajemnicy państwowej (art. 265 k.k.), obrażanie uczuć religijnych (art. 196 k.k.), rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody (art. 191 k.k.), groźba karalna (art. 190 k.k.), uporczywe nękanie (art. 190a k.k.), a także stręczycielstwo poprzez przekaz internetowy i czerpanie z tego tytułu korzyści majątkowych (art. 204 k.k.). Ponadto przy użyciu przekazu internetowego możliwe jest popełnienie przestępstwa zniesławiania (art. 212 k.k.), bądź zniewagi (art. 216 k.k.).

Dla sprawcy dopuszczającego się większości z tych przestępstw, internet jest jedynie narzędziem, środkiem służącym do popełnienia przestępstwa. Nie wszystkie z występków popełnionych przy użyciu komputerów godzą w prywatność. Niewątpliwie z naruszeniem prywatności wiąże się *hacking*

80 Wśród nich nieuprawniony dostęp do informacji (hacking) (art. 267 § 1 k.k.), nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych (art. 267 § 2 k.k.), nielegalny podsłuch i inwigilacja za pomocą urządzeń technicznych (art. 267 § 3 k.k.), ujawnianie informacji uzyskanych nielegalnie (art. 267 § 4 k.k.), naruszenie integralności zapisu informacji (art. 268 § 2 i 3 k.k.), niszczenie danych informatycznych (art. 268 a k.k.), sabotaż komputerowy (art. 269 k.k.), zakłócanie pracy systemu komputerowego lub sieci informatycznej (269a k.k.), bezprawne wykorzystanie programów i danych (art. 269 b k.k.).

81 Nielegalne uzyskanie programu komputerowego w celu osiągnięcia korzyści majątkowej (art. 278 § 2 k.k.), paserstwo programu komputerowego (art. 293 § 1 k.k.), oszustwo komputerowe (art. 287 k.k.), oszustwo telekomunikacyjne tj. kradzież impulsów telefonicznych (art. 285 k.k.).

82 Fałszerstwo komputerowe (art. 270 k.k.), niszczenie lub pozbawianie mocy dowodowej dokumentu elektronicznego (art. 276 k.k.), wyłudzenie (art. 297 § 1 k.k.), nierzetelne prowadzenie dokumentacji gospodarczej (art. 303 k.k.), fałszowanie kart płatniczych (art. 310 k.k.).

(nieuprawniony dostęp do informacji)[83], a także nielegalny podsłuch i inwigilacja przy pomocy urządzeń technicznych i programów komputerowych. Podkreślenia wymaga, że „siła rażenia" przekazu komputerowego jest znacznie szersza i dotkliwsza niż działanie za pomocą metod „tradycyjnych", tj. przekazu osobistego, a nawet informacji w prasie drukowanej bądź za pośrednictwem radiofonii, bądź telewizji. Sytuacja ta dotyczy zwykle zniesławień i zniewag, które z sadystyczną wręcz lubością zamieszczają użytkownicy rozmaitych for internetowych i portali społecznościowych. To właśnie w internecie napotkać można przejawy mowy nienawiści, odwołującej się do sądów, przekonań i ocen w utrwalonych stereotypach[84].

Zakończenie

Polskie rozwiązania legislacyjne odpowiadają zasadniczo rzecz biorąc wymogom systemu prawa unijnego, uniwersalnego, a także systemu Rady Europy. Niemniej podobnie jak wspomniane regulacje międzynarodowe nie do końca nadążają za szybkim postępem techniki, rozwojem sieci i wyzwaniami, jakie niesie ona za sobą. Wciąż pojawiają się nowe w większym lub mniejszym stopniu sprzeczne z obowiązującym prawem czyny obnażające jednocześnie niedoskonałość przyjętych regulacji. Proces ten wydaje się nieuchronny. Prowadzi on do niezwykle pesymistycznych wniosków, gdyż w ślad za czynami naruszającymi stabilność społeczną pojawiają się coraz silniejsze głosy, żądające kontroli przekazu w celu powstrzymania zjawisk wysoce negatywnych społecznie. Mowa nienawiści, towarzyszące jej fake newsy to tylko przykłady działań wysoce dolegliwych dla jednostek a niebezpiecznych dla grup społecznych. Znacznie groźniejsze może być przewidywane zjawisko cyberwojny bądź rozmaite typy zachowań godzące w struktury gospodarcze. Niestety rzeczywistość wydaje się potwierdzać konstatacje niektórych myślicieli, że ludzie

83 Szczegółową analizę technicznych aspektów hackingu przynosi doskonała monografia F. Radoniewicza, *Odpowiedzialność karna za hacking*..., s. 74–118. Zwrócić w tym miejscu wypada szczególniejszą uwagę na używane przez hackerów metody, wśród których szczególnie istotne wydają się tzw. socjotechnika lub inżynieria społeczna *(social engineering)*, polegająca na uzyskiwaniu poufnych informacji poprzez interakcje z ludźmi oraz *phising* (*password harvesting fishing)*, czyli uzyskiwanie poufnych danych poprzez podszywanie się pod podmioty i instytucje znane i zaufane.

84 Zob. w tym przedmiocie: R. Wieruszewski, M. Wyrzykowski, A. Bodnar, A. Gliszczyńska-Grabias, *Mowa nienawiści*..., S. Kowalski, M. Tulli, *Zamiast procesu. Raport o mowie nienawiści*, Warszawa 2003, s. 21 i n.

niekoniecznie z natury są dobrzy, gdyż znaczący odsetek wśród nich stanowią jednostki powodowane chęcią odwetu na społeczeństwie lub na jego wybranych przedstawicielach za poniesione porażki, niepowodzenia i klęski.

Bibliografia

Aleksandrowicz T., *Współczesny terroryzm międzynarodowy – próba definicji ze stanowiska prawa międzynarodowego*, „Wojskowy Przegląd Prawniczy" 2003, nr 2.

Andreski S., *Maksa Webera olśnienia i pomyłki*, Warszawa 1992.

Barman Z., *Globalizacja*, Warszawa 2000.

Becker J. (red.), *The Soviet Union and Terrorism*, London 1984.

Bell D., *The Coming of Post-Industial Society*, New York 1973.

Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2.

Bickerton P., Bickerton M., Pardesi U., *Marketing w internecie*, Gdańsk 2006.

Bieńkowska E., Mazowiecka L. (red.), *Dyrektywa Parlamentu Europejskiego i Rady ustanawiająca normy minimalne w zakresie praw wsparcia i ochrony ofiar przestępstw. Komentarz*, Warszawa 2014.

Boszczyk M., *Media elektroniczne jako środek komunikowania politycznego* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym*, Sosnowiec 2006.

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problem bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

Brink D.O., *Millian Principles, Freedom of Speech, and Hate Speech*, „Legal Theory" 2001, no. 7.

Clark I., *Globalization and International Relation Theory*, Oxford 1999.

Cline R.S., *Yonah Alexander: The Soviet Connection*, New York 1984.

Cohen-Almagor R., *Holocaust Denial is a Form of Hate Speech*, „The Amsterdam Law Forum" 2009, no. 2.

Cortese A., *Opposing hate speech*, Westport 2006.

Doktorowicz K., *Europejska droga do społeczeństwa informacyjnego* [w:] K. Doktorowicz (red.), *Społeczeństwo informacyjne. Wyzwania dla gospodarki, polityki i kultury*, Katowice 2002.

Doktorowicz K., *Europejski model społeczeństwa informacyjnego*, Katowice 2005.

Fleming M., *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy" 1996, nr 1.

Ghanea N., *Expression and Hate Speech in the ICCPR: Compatible or Clashing?*, „Religion and Human Rights" 2010, no. 5.

Gilarka K., *Państwo narodowe a globalizacja – dynamika powstawania nowego ładu*, Toruń 2003.

Gliszczyńska-Grabias A., *Międzynarodowoprawne standardy wolności a mowa nienawiści* [w:] D. Bychawska-Sinarska, D. Głowacka (red.), *Mowa nienawiści w internecie: jak z nią walczyć?*, Warszawa 2013.

Goban-Klas T., *Społeczeństwo informacyjne i jego teoretycy* [w:] J. Lubacz (red.), *W drodze do społeczeństwa informacyjnego*, Warszawa 1990.

Gołda-Sobczak M., *Spór o definicję terroryzmu*, „Wiedza i Umiejętności" 2004.

Grewlich K.W., *„Cyberspace". Sector – specyfic. Regulatio and Competition Rules in European Telecommunications*, „Common Market Law Review" 1999, nr 6.

Gruchoła M., *Ochrona użytkowników Internetu w państwach Unii Europejskiej*, Lublin 2012.

Grzybczyk K., *Twórczość internautów w świetle regulacji prawa autorskiego na przykładzie fanfiction*, Warszawa 2015.

Gulda P., *Elektroniczna demokracja – teoria i praktyka, wady i/lub zalety* [w:] M. Sokołowski (red.), *U progu wielkiej zmiany? Media w kulturze XXI wieku*, Olsztyn 2005.

Gulda P., *Internet jako przestrzeń polityczna* [w:] M. Sokołowski (red.), *Edukacja medialna. Nowa generacja pytań i obszarów badawczych*, Olsztyn 2004.
Hanusek T., *W sprawie pojęcia współczesnego terroryzmu*, „Problemy Kryminalistyczne" 1980, nr 143.
Hare I., Weinstein J. (red.), *Extreme Speech and Democracy*, Oxford 2009.
Hoeren T., *Werberecht im Internet am Beispiel der ICC Guidelines on Interactive Marketing Communications* [w:] M. Lehmann (red.), *Internet – und Multimediarecht (Cyberlaw)*, Stuttgart 1997.
Hoffman B., *Low-intensity Conflict: Terrorism and Guerrilla War fare in the Coming Decades* [w:] L. Howard (red.), *Terrorism: Roots, Ompact, Responses, Praegor*, New York 1992.
Hoffman B., *Oblicza terroryzmu*, Warszawa 2001.
Indecki K., *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź 1998.
Jaskuła L.K., *Wolność działalności dziennikarskiej w perspektywie zjawiska mowy nienawiści. Wybrane aspekty prawne* [w:] W. Lis (red.), *Status prawny dziennikarza*, Warszawa 2014.
Kasińska-Metryka, *Demokratyzacja systemu politycznego a przepływ informacji – od deficytu do przesytu* [w:] M. Sokołowski (red.), *U progu wielkiej zmiany? Media w kulturze XXI wieku*, Olsztyn 2005.
Kerr C., Dunlap J.T., Harbison F.H., Myers C.A., *Industrialism and Industirial Man*, Cambridge 1960.
King M., *Globalization, Knowledge and Society*, New York 1990.
Korcz I., *Internet a człowiek w kontekście globalizującego się świata?* [w:] M. Sokołowski, M. Furmanek (red.) *Oblicza Internetu. Internet a globalne społeczeństwo informacyjne*, Elbląg 2005.
Korzińska A., *Tradycja i nowoczesność. Islam w Internecie. Analiza polskojęzycznych stron internetowych* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI*, Elbląg 2006.
Kosiński J., *Cyberprzestępczość* [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak, (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013.
Kotarski H., *Internet a lokalna polityka. Studium socjologiczne na przykładzie wyborów samorządowych* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006.
Kowalski S., Tulli M., *Zamiast procesu. Raport o mowie nienawiści*, Warszawa 2003.
Lach A., *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015.
Laqueur W., *Terrorism*, London 1997.
Laqueur W., *The Age of Terrorism*, Boston 1987.
Łęski Z., Wieczorek Z., *Społeczeństwo wirtualne – czy mamy jakiś wybór?* [w:] M. Sokołowski, M. Furmanek (red.), *Oblicza Internetu. Internet a globalne społeczeństwo informacyjne*, Elbląg 2005.
Łętowska E., *Zwodnicze pokusy karania hate speech* [w:] D. Bychawska-Siniarska, D. Głowacka (red.), *Mowa nienawiści w internecie: jak z nią walczyć?*, Warszawa 2013.
Marschall A.M., Tompset B.C., *Identity theft in an online world*, „Computer Law and Security Report" 2005, nr 21.
Mason S., *Validating identity for the electronic environment*, „Computer Law and Security Report" 2004, nr 3.
Matusiak I., *Gra komputerowa jako przedmiot prawa autorskiego*, Warszawa 2013.
Muszyński W., *Wizerunek polskich tradycjonalistów Internecie* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI*, Elbląg 2006.
Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, nr 3.
Pala M., *Wybrane aspekty bezpieczeństwa w cyberprzestrzeni*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, nr 1.
Pawłowski A., *Terroryzm w Europie w XIX i XX wieku*, Zielona Góra 1980.

Pietras M., *Globalizacja jako proces zmian społeczności międzynarodowej* [w:] M. Pietras (red.), *Oblicza procesów globalizacji*, Lublin 2002.
Pikulski S., *Prawne środki zwalczania terroryzmu*, Olsztyn 2000.
Preis E., *Glosa do wyroku Trybunału Sprawiedliwości z dnia 29 stycznia 2008, C – 275/06*, „Europejski Przegląd Sądowy" 2009, nr 4.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
Rinaldi A.H. *Internationale Netze und das Wettberbstrecht* [w:] J. Becker (red.) *Rechtsprobleme internationalen Dattenetze*, Baden-Baden 1996.
Sauer A., *Online privacy and the online self*, „Privacy Law Bulletin" 2008, nr 9.
Schittek G., *Internet jako narzędzie politycznego wsparcia w Szwecji* [w:] T. Zasępa (red.), *Internet. Fenomen społeczeństwa informacyjnego*, Częstochowa 2001.
Schmid A.P., *Political Terrorism: A Research Guide*, New Brunswick 1984.
Scholte J.A., *The Globalization of World Politics* [w:] J. Baylis, S. Smith (red.), *The Globalization of World Politics. An Introduction to International Relations*, New York 2001.
Serwiak S., *Cyberprzestrzeń jako źródło zagrożenia terroryzmem* [w:] E. Pływaczewski (red.), *Przestępczość zorganizowana, świadek koronny i terroryzm w ujęciu praktycznym*, Kraków 2005.
Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni* [w:] T. Jemioło, J. Kisielniecki, K. Rajchel (red.), *Cyberterroryzm – nowe wyznawania XXI wieku*, Warszawa 2009.
Sobczak J., *Dylematy społeczeństwa informacyjnego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI wieku*, Elbląg 2006.
Sobczak J., *Europejski ład komunikacyjny w procesie globalizacji* [w:] J. Sobczak, R. Bäcker, *Europejska myśl polityczna wobec globalizacji*, Łódź 2005.
Sobczak J., Kakareko K., *Odpowiedzialność za przestępstwa popełnione w sieci, a kwestia prywatności* [w:] J. Sobczak, K. Chałubińska-Jentkiewicz, K. Kakareko, *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017.
Sobczak J., *Problemy społeczeństwa informacyjnego w dobie globalizacji* [w:] T. Wallas (red.), *Bariery rozwoju na progu XXI wieku. Wybrane problemy*, Warszawa 2007.
Sobczak J., *Społeczeństwo informacyjne w dobie globalizacji* [w:] M. Domagała, J. Iwanek, *Demokracja w dobie globalizacji*, t. II, *Aspekty teoretyczne*, Katowice 2008.
Sobczak J., *Wolność słowa a zjawisko inwigilacji przekazu internetowego* [w:] M. Sokołowski (red.), *Oblicza Internetu. Architektura komunikacyjna sieci*, Elbląg 2007.
Sobczyk S., *Internet narzędziem oddziaływania na wyborców* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006.
Stammers N., *Social movements and the challenge to power* [w:] M. Shaw (red.), *Politics in Globalized Word*, London 1999.
Śledzińska-Simon A., *Decyzja ramowa w sprawie zwalczania pewnych form przejawów rasizmu i ksenofobii jako trudny kompromis wobec mowy nienawiści w Unii Europejskiej* [w:] R. Wieruszewski, M. Wyszykowski, A. Bodnar, A. Gliszczyńska-Grabias (red.), *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010.
Turska A., *Marketing polityczny w Internecie* [w:] S. Michalczyk (red.), *Media i komunikowanie w społeczeństwie demokratycznym. Szkice medioznawcze*, Sosnowiec 2006.
Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego. Studia i Analizy" 2013, nr 9.
Weber M., *Gospodarka i społeczeństwo. Zarys socjologii rozumiejącej*, Warszawa 2002.
Wieruszewski R., Wyrzykowski M., Bodnar A., Gliszczyńska-Grabias A., *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010.
Woiński M., *Prawnokarne aspekty zwalczania mowy nienawiści*, Warszawa 2014.
Wójcik J.W., *Przeciwdziałania finansowaniu terroryzmu*, Warszawa 2007.

Zacher L.W., *Etykietowanie przyszłych społeczeństw – kryteria, określenia, ewaluacje* [w:] M. Sokołowski (red.), *U progu wielkiej zmiany? Media w kulturze XXI wieku*, Olsztyn 2005.
Zasępa T., *Komunikacja cybernetyczna wyzwaniem dla Kościoła katolickiego* [w:] T. Zasępa (red.), *Internet i nowe technologie – ku społeczeństwu przyszłości*, Częstochowa 2003.

Cybercrime between Polish and international regulations

Abstract

The article presents the problem of cybercrime, regulated by national and international regulations. In the era of information society where the internet plays an important role and where the number of its users is constantly growing, the law is often infringed which often leads to crimes. Crimes in cyberspace, understood as a communication area created by the system of internet connections, are getting more and more serious and more and more difficult to detect and investigate. National regulations, as well as international ones, not always keep up with the dynamic technological progress, network development and many challenges it poses. New offences, that appear in the cyberspace and that are more or less contrary to the applicable law, are still committed which exposes the weaknesses of the adopted regulations.

Key words: crime, cyberspace, information society, national law, international law, threat, cyberterrorism, cyberattack, security system

Filip Radoniewicz*

Przestępstwa komputerowe w polskim Kodeksie karnym

Streszczenie

Celem artykułu jest analiza przepisów kryminalizujących w polskim prawie zjawisko tzw. przestępstw komputerowych w rozumieniu ścisłym (computer crimes, cybercrimes), czyli takich czynów, w których komputer lub sieć są celem przestępstwa (niejako „ofiarą"; *computer as a target*). Artykuł składa się z trzech części – wstępu, w którym w sposób syntetyczny omówiono najważniejsze kwestie terminologiczne, części głównej, w której przeprowadzono analizę przepisów art. 267–269c Kodeksu karnego z 1997 r., znajdujących się w rozdziale XXXIII, zatytułowanym *Przestępstwa przeciwko ochronie informacji*, w których polski ustawodawca przestępstwa te stypizował oraz zakończenia zawierającego uwagi de lege lata i de lege ferenda.

Słowa kluczowe: cyberprzestępczość, hacking, narzędzia hackerskie, inwigilacja, podsłuch komputerowy

* Dr Filip Radoniewicz, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

Wstęp

Dotychczas w żadnym ustawodawstwie nie zdefiniowano pojęcia, „przestępstwa komputerowego". Oczywiście w nauce prawa karnego nie brakuje definicji tego terminu. Jako jedną z pierwszych można wskazać niezwykle szeroką i pojemną definicję „przestępstwa komputerowego" zaproponowaną przez Ulricha Siebera na spotkaniu ekspertów OECD w Paryżu w 1983 r., użytą następnie w tzw. Raporcie OECD[1], zgodnie z którą „za przestępstwo komputerowe uważa się wszelkie bezprawne, nieetyczne i nieupoważnione zachowania odnoszące się do procesu przetwarzania i (lub) przekazywania danych"[2] . Bardzo ogólną definicję przestępczości komputerowej sformułowano kilka lat później dla potrzeb Interpolu, określając ją jako „przestępczość w zakresie technik komputerowych" i dzieląc na następujące grupy: 1) naruszenie praw dostępu do zasobów; 2) oszustwo przy użyciu komputera; 3) modyfikacja zasobów komputera; 4) powielanie programów; 5) sabotaż sprzętu i oprogramowania; 6) przestępstwa dokonywane za pomocą BBS-ów; 7) przechowywanie zabronionych prawem zbiorów; 8) przestępczość w internecie[3].

W związku z postępem technologicznym ewoluują również pojęcia określające zjawisko przestępczości komputerowej. Najwcześniejsze to oczywiście „przestępstwo komputerowe" (ang. *Computer crime*), „przestępstwo związane z komputerem" (ang. *Computer related crime*), „przestępstwo popełniane za pomocą komputera" (ang. *crime by computer*), „przestępstwo związane z technologią cyfrową" (ang. *Digital crime*; zakres tego pojęcia jest szerszy niż „przestępstwo komputerowe"). Natomiast rozwój internetu w ostatnich latach doprowadził do powstania silnego, praktycznie nierozerwalnego związku między technologią informatyczną i telekomunikacyjną. Dlatego też pojawiło się wiele nowych propozycji terminów i definicji na określenie zjawiska przestępstw komputerowych. Wskazać można „przestępstwa internetowe" (ang. *internet crimes*), „e-przestępstwa" (ang. *e-crimes*), „przestępstwa sieciowe" (ang. *net-crimes*), „wirtualne" (ang. *Virtual crimes*) i wreszcie „cyberprzestępstwa" (ang.

1 Computer-Related Crime. Analysis of legal policy in the OECD Area ICCP Series nr 10, OECD, Paryż 1986. Dokument zawierający wyniki podjętych przez OECD w 1983 r. badań nad możliwością stworzenia międzynarodowych regulacji prawnokarnych dotyczących przestępstw i nadużyć komputerowych.

2 U. Sieber, *Legal Aspects of Computer-Related Crime in the Information Society – Comcrime – Study*, Würzburg 1998, s. 20–21; por. R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*, Warszawa 1993, s. 52.

3 B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000, s. 27–28.

Cyber crimes), „przestępstwa związane z technologią informatyczną" (ang. *IT-crimes*), „przestępstwa związane z przetwarzaniem danych"[4]. Wśród przestępstw komputerowych wyróżnić można pewne grupy: 1) przestępstwa, które nie wymagają, by komputer był podłączony do sieci – obecnie zdarzające się stosunkowo rzadko; 2) przestępstwa, które można popełnić wyłącznie w internecie (przestępstwa internetowe, wirtualne); 3) przestępstwa generalnie związane z nowoczesną technologią, czyli te, które związane są z komputerami i sieciami komputerowymi, ale dotyczą również nanotechnologii czy bioinżynierii[5].

Sformułowaniem, które robi największą karierę, jest zdecydowanie termin „cyberprzestępstwo", używany zarówno w literaturze przedmiotu, jak i w niektórych dokumentach międzynarodowych (w szczególności w Konwencji o cyberprzestępczości).

Na X Kongresie ONZ w sprawie zapobiegania przestępczości i postępowania z przestępcami (*The Tenth United Nation Congress on the Prevention of Crime and Treatment of Offenders*), który odbył się w kwietniu 2000 r. w Wiedniu, uznano, że cyberprzestępstwem jest każde przestępstwo, które może być popełnione za pośrednictwem systemów komputerowych lub sieci, w systemie komputerowym lub sieci albo przeciwko takiemu systemowi lub sieci. Jednocześnie zaproponowano następujący podział cyberprzestępstw: 1) cyberprzestępstwo w wąskim ujęciu (przestępstwo komputerowe): każde nielegalne działanie wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych i przetwarzanych przez te systemy danych, tj.: a) nieautoryzowany dostęp, b) uszkodzenie komputera, danych lub aplikacji, c) sabotaż komputerowy, d) nieautoryzowane przejęcie komputera, e) szpiegostwo komputerowe; 2) cyberprzestępstwo w szerokim ujęciu (przestępstwo dotyczące komputerów): każde nielegalne działanie dokonane za pomocą lub dotyczące systemów komputerowych lub sieci komputerowych, włączając w to m.in. nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[6].

4 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 32–33. Por. B. Fischer, *Przestępstwa komputerowe...*, s. 23–31; J.W. Wójcik, *Przestępstwa komputerowe. Fenomen cywilizacji*, cz. I, Warszawa 1999, s. 52–57; J. Clough, *Principles of Cybercrime*, New York 2013, s. 9.

5 J. Clough, *Principles of cybercrime...*, s. 9.

6 Por. M. Smarzewski, *Cyberprzestępczość a zmiany w polskim prawie karnym* [w:] I. Sepioło-Jankowska (red.), *Reforma prawa karnego. Księga po Zjeździe Młodych Karnistów*, Warszawa 2014, s. 267; D.L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004, s. 35–36.

W literaturze stworzono wiele klasyfikacji przestępstw komputerowych. Z uwagi na ograniczenia objętościowe ograniczę się do wskazania dwóch. Po pierwsze najprostszego z możliwych podziału dychotomicznego przestępstw komputerowych na „stare" i „nowe" występki. Przy czym chodzi tu o „nowość" przestępstwa w ogóle (a nie jako przestępstwa komputerowego). Pierwsza grupa to przestępstwa konwencjonalne (pospolite), które dzięki rozwojowi techniki uzyskały nową lub zmodyfikowaną postać (np. oszustwo, nękanie czy rozpowszechnianie pornografii dziecięcej). „Nowe" przestępstwa to te, które pojawiły się w związku z powstaniem komputerów, a następnie rozwojem technologii informatycznej i jej konwergencji z telekomunikacją. Klasycznym przykładem będzie uzyskanie nieuprawnionego dostępu czy nieuprawniona modyfikacja danych komputerowych[7]. Po drugie najpowszechniejszego i najbardziej praktycznego (bo najmniej wysublimowanego i najbardziej odpowiadającego rzeczywistości) podziału na przestępstwa, w których: 1) komputer lub sieć są celem przestępstwa (niejako „ofiarą"; *computer as a target*), inaczej po prostu *computer crimes*, np. hacking, podsłuch komputerowy, zakłócanie pracy sieci – przestępstwa będące przedmiotem niniejszego artykułu; 2) komputer lub sieć są narzędziem przestępstwa (*computer as an instrument or a tool*), inaczej *computer related crimes*, np. rozpowszechnianie pornografii dziecięcej, oszustwo[8]; 3) komputer lub sieć mogą być użyte do zadań dodatkowych, związanych z popełnieniem przestępstwa (np. do przechowywania danych o nielegalnej sprzedaży narkotyków)[9].

Zarówno w literaturze, jak i w ustawodawstwach można znaleźć zbliżony do powyższego „trójpodział" cyberprzestępstw[10] na: przestępstwa kompute-

7 Por. np. P. Grabosky, *Electronic Crime*, New Jersey 2006, s. 12–14.

8 Często spotykane jest rozbicie tej kategorii na dwie grupy: *computer assisted (related) crimes* – przestępstwa związane z użyciem komputera, takie jak oszustwo komputerowe, oraz *computer content crimes* – cyberprzestępstwa związane z treścią przetwarzanej informacji, takie jak np. rozpowszechnianie pornografii dziecięcej. Zob. np. B.J. Koops, T. Robinson, *Cybercrime Law: A European Perspective* [w:] E. Casey (red.), *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, Waltham–San Diego–London 2011, s. 130–133; D. Wall, *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013, s. 49–50.

9 S. Brenner [w:] R.D. Clifford (red.), *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime*, Durham 2011, s. 17–20; J. Clough, *Principles of cybercrime...*, s. 10, P. Grabosky, *Electronic crime...*, s. 11.

10 J. Clough, *Principles of cybercrime...*, s. 10. Por. K. Dudka, *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin 1998, s. 105. Na temat klasyfikacji przestępstw komputerowych zob. też: J. Kosiński, *Cyberprzestępczość...*, s. 463–465; M. Siwicki, *Definicje i podział cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 241–252; M. Smarzewski,

rowe (ang. *Computer crimes*), przestępstwa, których popełnienie jest umożliwiane przez komputery (ang. *Computer facilitated crimes*), i przestępstwa, których popełnienie jest wspierane przez komputery (ang. *Computer supported crimes*).

Powyższy trójpodział przyjęty jest również w Konwencji o cyberprzestępczości[11] jedynej umowie międzynarodowej dotyczącej zwalczania przestępstw popełnianych za pośrednictwem internetu oraz sieci komputerowych. Przestępstwa odpowiadające czynom zabronionym z pierwszej grupy zostały w niej zebrane w jednym tytule jako *Przestępstwa przeciwko poufności, integralności i dostępności danych komputerowych i systemów komputerowych*. Natomiast przestępstwa z drugiej grupy znalazły się w trzech kolejnych tytułach jako *Przestępstwa związane z komputerami*, *Przestępstwa związane z treścią* oraz *Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych*.

Ostatnia grupa z „trójpodziału" nie jest przedmiotem zainteresowania prawa karnego materialnego, ale raczej procesowego, a zwłaszcza dowodowego. Dlatego też omawiając problematykę przestępstw komputerowych, pozostawia się je zwykle z boku.

Przestępstwa komputerowe w kodeksie karnym z 1997 r.

Polska regulacja czynów zabronionych określonych w dyrektywie 2013/40 znajduje się w rozdziale XXXIII Kodeksu karnego[12] „Przestępstwa przeciwko ochronie informacji", w przepisach art. 267–269c. Swój obecny kształt zawdzięcza ona trzem nowelizacjom: pierwszej, przeprowadzonej ustawą z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń[13], mającej dostosować polskie przepisy do postanowień wspomnianej Konwencji o cyberprzestępczości, drugiej, dokonanej ustawą z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw[14], której celem była implementa-

Cyberprzestępczość a zmiany w polskim prawie karnym [w:] I. Sepioło-Jankowska (red.), *Reforma prawa karnego. Księga po Zjeździe Młodych Karnistów*, Warszawa 2014, s. 264–267.

11 Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).

12 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2016 r., poz. 1137 ze zm.), dalej jako k.k.

13 Dz.U. nr 69, poz. 626.

14 Dz.U. nr 214, poz. 1344.

cja decyzji ramowej 2005/222/WSiSW w sprawie ataków na systemy informatyczne[15] oraz trzeciej, przeprowadzonej ustawą z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw[16], której głównym celem było wdrożenie dyrektywy 2014/42/UE z dnia 3 kwietnia 2014 r. w prawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej[17] oraz – „częściowo" (jak to określono w ustawie) – dyrektywy 2013/40 dotyczącej ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW[18].

W treści art. 267 § 1 k.k. przewidziano odpowiedzialność karną za uzyskanie przez sprawcę bez uprawnienia dostępu do informacji[19] dla niego nieprzeznaczonej. Dokonano w nim kryminalizacji trzech czynów, będących zamachami na bezpieczeństwo systemów informatycznych i przetwarzanych w nich danych.

15 Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 69, s. 67).

16 Dz.U. z 2017 r., poz. 768.

17 Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w prawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz.Urz. UE L 127, s. 39).

18 Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218, s. 8).

19 Należy już na wstępie zwrócić uwagę, iż w aktach prawa międzynarodowego oraz unijnego dotyczących problematyki bezpieczeństwa sieci komputerowych dla określenia przedmiotu ochrony operuje się pojęciem „danych komputerowych", a nie „informacji". Polski ustawodawca pojęcia informacji i danych w zasadzie utożsamia, mimo zachodzących między nimi różnic. W świetle przepisu art. 2 lit b dyrektywy 2014/30 „dane komputerowe" należy rozumieć jako „przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym wykonanie funkcji przez system informatyczny". Zbliżona definicja znajduje się w Konwencji o cyberprzestępczości. Zgodnie z powyższym dane komputerowe są nośnikiem (medium) informacji, faktów i koncepcji, które dopiero sprowadzone do postaci danych komputerowych są czytelne dla systemu komputerowego (czy informatycznego). W zakres tego pojęcia wchodzą również programy komputerowe. Rozróżnienie pojęć „danych komputerowych" i „informacji" ma znaczenie z prawnego punktu widzenia. Można bowiem wejść w posiadanie danych komputerowych, ale nie móc skorzystać z zawartych w nich informacji np. z uwagi na nieznajomość algorytmu, według którego zostały one zakodowane. Zniszczenie danych nie zawsze oznacza zniszczenie informacji, podobnie jak zabór danych nie musi być kradzieżą informacji. Zob. szerzej: A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 37 i n.

Po pierwsze – podłączenia się do sieci telekomunikacyjnej[20], czyli uzyskanie fizycznego dostępu do niej np. poprzez podłączenie się przez sprawcę za jej pośrednictwem do serwera i uzyskanie dostępu do przechowywanych w nim danych (działania polegające na ich przechwytywaniu w trakcie przesyłania penalizuje art. 267 § 3 k.k.).

Po drugie – uzyskania dostępu do informacji w wyniku przełamania elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia. Chronione są zatem jedynie informacje przechowywane w systemach komputerowych, które zostały przez ich dysponenta zabezpieczone przed nieuprawnionym dostępem. Pod pojęciem elektronicznego, magnetycznego, informatycznego zabezpieczenia należy rozumieć „wszelkie formy utrudnienia dostępu do informacji, których usunięcie wymaga wiedzy specjalistycznej lub posiadania szczególnego urządzenia lub kodu"[21], natomiast „inne szczególne zabezpieczenie" jest kategorią dopełniającą, obejmującą środki niemożliwe do zakwalifikowania do któregoś z określonych w przepisie rodzajów, a których zniwelowanie sprawia sprawcy co najmniej takie trudności, jak przełamanie zabezpieczenia elektronicznego, magnetycznego lub informatycznego[22]. Dane komputerowe mogą być chronione bezpośrednio,

20 Zgodnie z definicją zawartą w przepisie art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2016 r., poz. 1489 ze zm.) przez sieć telekomunikacyjną należy rozumieć „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju". Będą to zatem np. sieci satelitarne, sieci stałe wykorzystujące komutację łączy (ang. *Circuit switching*, inaczej komutacja kanałów lub komutacja obwodów – polega na tworzeniu na żądanie między dwiema lub większą ilością punktów sieci „stałego" połączenia do ich wyłącznego użytku na czas transmisji) oraz komutację pakietów (ang. *Packet switching*– sposób transmisji danych polegający na podziale ich na pakiety, z których każdy może dotrzeć inną drogą do celu; proces przesyłania pakietów nazywa się routowaniem lub trasowaniem i odbywa się pomiędzy węzłami sieci – routerami), sieci telewizji kablowej czy sieci elektryczne umożliwiające transmisję sygnałów. Urządzenia komutacyjne to urządzenia służące komutacji łączy (np. centrale telefoniczne), natomiast urządzenia przekierowujące – komutacji pakietów (będą to przede wszystkim routery). Zob. szerzej: A. Krasuski, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010, s. 83–84; S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013, s. 82–83; F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko komputerowym i systemom informatycznym*, Warszawa 2016, s. 278–282.

21 W. Wróbel [w:] A. Zoll (red.), *Kodeks karny. Komentarz. Część szczególna. Komentarz do artykułów 117–277 k.k.*, t. II, Warszawa 2013, s. 1502.

22 P. Kardas *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1, s. 71.

np. przez zaszyfrowanie czy zabezpieczenie dostępu hasłem, lub pośrednio – w ramach ochrony samego systemu informatycznego – czemu służą *firewalle*, systemy wykrywania włamań czy procedura uwierzytelniania. „Przełamaniem zabezpieczeń" jest bezpośrednie oddziaływanie sprawcy na zabezpieczenie, prowadzące do zniwelowania jego funkcji ochronnej, które nie musi się wiązać z jego zniszczeniem[23]. W doktrynie podkreśla się, że ma być ono realne oraz aktywne w momencie popełnienia czynu. W przeciwnym wypadku nie dojdzie do wypełnienia znamion przestępstwa[24].

Po trzecie – ominięcia wskazanych wyżej zabezpieczeń i uzyskanie dzięki temu dostępu do informacji. Nie należy bowiem zapominać, że przełamanie zabezpieczeń jest tylko jedną z wielu technik (i to nawet nie najczęściej stosowaną) używanych przez hackerów do penetracji systemów komputerowych. Pozostałe sprowadzają się do ich ominięcia, a polegają na wprowadzeniu w błąd człowieka (*social engineering*, czyli tzw. socjotechnika, polegająca np. na wyłudzeniu hasła), wprowadzeniu w błąd systemu (np. tzw. *IP spoofing*, czyli fałszowanie adresów, mające na celu wprowadzenie w błąd co do miejsca wysłania pakietów danych) czy wykorzystaniu luk (błędów) lub słabości w systemach operacyjnych, aplikacjach, czy protokołach (zbiorach zasad określających procesy komunikacyjne odpowiadające m.in. za identyfikację komputerów w sieci), czemu służą programy zwane *exploitami*.

W przepisie art. 267 § 2 k.k. dokonano kryminalizacji nieuprawnionego uzyskania dostępu do całości lub części systemu informatycznego[25]. Autorzy

23 P. Kardas, *Prawnokarna ochrona...*, s. 71–72; P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks karny. Praktyczny komentarz*, Warszawa 2012, s. 621; W. Wróbel [w:] A. Zoll (red.), *Kodeks*..., s. 1502–1503.

24 Por. S. Bukowski, *Przestępstwo hackingu*, „Przegląd Sądowy" 2006, nr 4, s. 142–143; P. Kardas, *Prawnokarna ochrona*..., s. 64.

25 Interpretacja tego pojęcia w zasadzie od momentu pojawienia się go w Kodeksie karnym rodziła problemy (zob. szerzej np.: F. Radoniewicz, *Odpowiedzialność karna*..., s. 275–278 oraz M. Siwicki, *Cyberprzestępczość*, Legalis 2013), które dodatkowo przybrały na sile po ratyfikacji przez Polskę Konwencji o cyberprzestępczości. Ponieważ przepis art. 267 § 2 k.k. dodany został nowelizacją z 2008 r., związaną z implementacją decyzji ramowej 2005/222, wskazane byłoby zatem rozumienie tegoż terminu, zgodnie z definicją zawartą w tym akcie oraz w zastępującej go dyrektywie 2013/40, a więc zarówno jako pojedyncze urządzenie przetwarzające dane komputerowe, jak i zespół takich urządzeń, czyli sieć (zob. wcześniejsze uwagi). Natomiast tłumacząc tekst Konwencji o cyberprzestępczości popełniono wiele błędów. Jednym z nich jest przetłumaczenie pojęcia systemu komputerowego (ang. *computer system*), jako systemu informatycznego. A jak wspominano wcześniej, zakres przedmiotowy pojęcia system komputerowy z Konwencji jest węższy niż „systemu informatycznego" z dyrektywy 2013/40. Powoduje to wątpliwości co do zakresu pojęcia systemu informatycznego na gruncie Kodeksu karnego. Należy jednocześnie zaznaczyć, że mimo

projektu nowelizacji z 2008 r. – którą dodano tenże przepis – słusznie wskazali w jej uzasadnieniu, że celem uzyskania nieuprawnionego dostępu do systemu może być nie tylko uzyskanie dostępu do informacji, których dane informatyczne są nośnikiem, ale stanowić może niejako wstęp do innych działań, np. powołanemu jako przykład w uzasadnieniu umieszczeniu w komputerze programu, umożliwiającego przejęcie nad nim kontroli, celem stworzenia botnetu[26], za pomocą którego sprawca ma zamiar przeprowadzić atak dDoS[27]. Przepis ten znajdzie zastosowanie, gdy celem sprawcy, który uzyskuje nieuprawniony dostęp jest popełnienie następnie „pospolitego" przestępstwa (zachowanie sprawcy może bowiem polegać np. na uzyskaniu dostępu do konta innego użytkownika w serwisie aukcyjnym, celem wykorzystania go do dokonywania oszustw) lub gdy działał z innych pobudek, takich jak np. sprawdzenie własnych umiejętności czy uzyskanie szacunku w „środowisku hackerskim". Tym samym cel, który sprawca miał zamiar osiągnąć czy motyw, jakim się kierował jest obojętny dla bytu przestępstwa stypizowanego w art. 267 § 2 k.k.

iż Konwencja o cyberprzestępczości w momencie jej ratyfikacji stała się częścią porządku prawnego, to definicji „systemu informatycznego" (komputerowego) nie można stosować bezpośrednio, z uwagi właśnie na omawiane problemy. Istniejący zamęt potęguje fakt, że w tłumaczeniu definicji pojęcia danych informatycznych w art. 2 lit. b Konwencji (ang. *Computer data*, przetłumaczonych jako „dane informatyczne") posłużono się pojęciem systemu komputerowego („dane informatyczne oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny"). Ponadto terminu „system komputerowy" użyto w tłumaczeniu Protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości dotyczącego penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych z dnia 28 stycznia 2003 r (Dz.U. z 2015 r., poz. 730).

26 Botnety, czyli sieci komputerów, na których sprawca (bez wiedzy ich użytkowników) zainstalował specjalne programy – tzw. zombie (stąd przejęte komputery nazywane są „komputerami-zombie"), które są zdalnie uruchamiane w określonym momencie w celu np. przeprowadzenia ataku dDoS. Ponieważ możliwe jest wykorzystanie ogromnej liczby komputerów (nawet kilkuset tysięcy, rozsianych po całym świecie), prawdziwe źródło ataku pozostaje nieznane. Obecnie w internecie można uzyskać zarówno programy do przeprowadzenia ataków DoS, jak i „gotowe" botnety do przeprowadzenia ataków dDoS. Botnety ponadto mogą być wykorzystywane np. do rozsyłania spamu (niechcianych wiadomości e-mail). Zob. szerzej np.: A. Adamski, *Botnety jako zagadnienie prawno-kryminologiczne na tle doświadczeń amerykańskich*, „Prokuratura i Prawo" 2013, nr 1, s. 68–69.

27 Ataki DoS (ataki odmowy usług, Denial of Service) mają zazwyczaj na celu zakłócenie pracy sieci (łącznie z jej zablokowaniem). W zasadzie można przyjąć, iż polegają na wywołaniu dużego ruchu sieciowego, prowadzącego do zawieszenia serwera, przeciążenia routera lub urządzeń sieciowych. Mogą być również skierowane przeciw konkretnym komputerom, uniemożliwiając im komunikację z serwerem. Ich „wzmocnionym" wariantem są ataki DdoS (rozproszone ataki DoS, *Distributed Denial of Service*), wykorzystujące *botnety*.

Przez dostęp do całości lub części zarówno systemu informatycznego należy rozumieć uzyskanie możliwości korzystania z jego zasobów, czyli – w zasadzie – przetwarzanych w nim danych, co jednak nie jest równoznaczne z dostępem do informacji, gdyż dane mogą być np. zaszyfrowane lub całkowicie niezrozumiałe dla sprawcy.

Przez dostęp nieuprawniony w rozumieniu niniejszego przepisu należy rozumieć dostęp bez uprawnień lub z ich przekroczeniem.

Rozwiązanie przyjęte przez ustawodawcę w przepisie art. 267 § 2 k.k. spotkało się z uzasadnioną krytyką z trzech zasadniczych powodów. Po pierwsze, jest to dosłowne przekopiowanie treści art. 2 decyzji ramowej 2005/222 („Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor"). Należy podkreślić, że decyzje ramowe służyły zbliżaniu przepisów prawnych państw członkowskich. Określały rezultat, jaki ma zostać osiągnięty, dobór środków ku temu prowadzących pozostawiając państwom członkowskim. W związku z tym ich postanowienia sformułowane są bardzo ogólnie. Decyzje ramowe harmonizujące prawo karne materialne nie nadają się zatem do dosłownej transpozycji. Po drugie przepis art. 267 § 2 k.k. jest niezwykle pojemny treściowo. Znamiona czynu w nim opisanego wypełni sprawca, który „uzyskuje nielegalny dostęp" do danych, bo na tym w zasadzie polega – o czym była już mowa – uzyskanie dostępu do systemu, przy czym by odpowiadać karnie, nie musi naruszyć zabezpieczenia. Jedynym warunkiem jest, by dostęp ów był nieuprawniony. Przyjąć należy, że przepis art. 267 § 2 k.k. będzie znajdował zastosowanie w przypadkach, gdy głównym elementem czynu sprawcy było uzyskanie dostępu do systemu informatycznego, a nie uzyskanie dostępu do informacji. Z sytuacją taką mamy do czynienia np. w wypadku włamania się do komputera w celu umieszczenia w nim bota. Szeroki zakres przedmiotowy przepisu art. 267 § 2 k.k. sprawia, że również część zachowań kryminalizowanych przez przepis art. 267 § 3 k.k., określanych jako podsłuch komputerowy, będzie mogła być jednocześnie kwalifikowana z art. 267 § 2 k.k. Uzyskanie nieuprawnionego dostępu do sieci jest równoznaczne z uzyskaniem dostępu do przesyłanych nią danych, tak więc sprawca realizuje jednocześnie znamiona czynu zabronionego z art. 267 § 3 k.k.

Po trzecie jedynym warunkiem, który musi zostać spełniony, aby możliwe było postawienie sprawcy zarzutu naruszenia przepisu art. 267 § 2 k.k., jest uzyskanie przez niego dostępu do systemu bez uprawnień. Kwestia praw dostępu do zasobów systemu informatycznego regulowana jest w większości

wypadków przez przepisy „miękkiego prawa" – regulaminy wewnętrzne sieci. Natomiast o nadaniu użytkownikowi uprawnień oraz o ich zakresie, decyduje administrator systemu. Takie odesłanie do norm pozaprawnych jest niebezpieczne i trudne do pogodzenia z zasadą określoności przestępstwa[28].

Ostatnią nowelizacją dodano przepis 269c, zgodnie z którym nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Narzędziem do walki m.in. z tzw. podsłuchem komputerowym[29] jest wspominany już kilkakrotnie artykuł 267 § 3 k.k., penalizujący zakładanie lub posługiwanie się – w celu uzyskania informacji[30] – podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

Należy podkreślić, że kryminalizuje on jedynie przechwytywanie danych komputerowych w czasie ich przesyłania. W przypadku uzyskania przez sprawcę danych przechowywanych np. na serwerze czy w prywatnym komputerze właściwa będzie kwalifikacja z art. 267 § 1 k.k. lub art. 267 § 2 k.k.

Bezprawność zachowania sprawcy zostaje oczywiście uchylona, jeśli zachowanie wypełniające znamiona jest legalnym działaniem organów ścigania (wynika z odpowiednich przepisów[31]).

28 Zob. szerzej: A. Adamski, *Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?*, „Prawo Teleinformatyczne" 2007, nr 3, s. 7–8; F. Radoniewicz, *Odpowiedzialność karna…*, s. 301–303.

29 Podsłuch komputerowy jest potocznym określeniem inwigilacji systemów informatycznych. Często nie w pełni poprawnie określa się to zjawisko mianem *sniffingu*, stanowiącego jedynie jedną z jego technik. Wyróżnia się dwa rodzaje podsłuchu komputerowego: pasywny – gdy sprawca jedynie zapoznaje się z treścią informacji oraz aktywny – gdy dokonuje modyfikacji przesyłanych danych, np. poprzez przekierowanie ich transmisji do innego miejsca w sieci.

30 Należy zwrócić uwagę, że dyrektywa 2013/40 nie przewiduje wymogu wystąpienia po stronie sprawcy przestępstwa nielegalnego przechwytywania danych jakichkolwiek dodatkowych wymogów dla przypisania mu odpowiedzialności karnej – np. „nieuczciwego" zamiaru, czy działania w określonym celu („Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor" – art. 6 dyrektywy 2013/40).

31 Przede wszystkim należy wskazać przepisy kodeksu postępowania karnego, ustawy z dnia 6 kwietnia 1990 r. o Policji (tj. Dz.U. z 2016 r., poz. 1782 ze zm.), ustawy z dnia 24 maja

W art. 268 § 2 k.k. dokonano kryminalizacji nieuprawnionej ingerencji w dane komputerowe, polegającej na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu zapisu istotnej informacji na informatycznym nośniku danych[32] oraz ograniczania ich dostępności dla osoby uprawnionej[33] poprzez udaremnianie lub znaczne utrudnianie w inny sposób zapoznanie się z informacją utrwaloną na takim informatycznym nośniku danych.

Informacja, będąca przedmiotem czynu sprawcy musi być „istotna", przede wszystkim w sensie obiektywnym (ze względu na jej treść, wagę i znaczenie[34]) – ale z uwzględnieniem interesów osoby uprawnionej do zapoznania się z nią[35], w tym celu, jakiemu służyła lub miała służyć[36].

Ponieważ przedmiotem ochrony jest „informacja zapisana na informatycznym nośniku danych", przepis art. 268 § 2 k.k. nie znajdzie zastosowania w sytuacji, gdy utrudnienie w zapoznaniu się z nią będzie wynikiem zakłócania pracy sieci (wówczas zachowanie sprawcy powinno zostać zakwalifikowane na podstawie art. 268a § 1 lub 2 albo 269a k.k.).

Typem kwalifikowanym tego przestępstwa jest czyn z art. 268 § 3 k.k. Znamieniem kwalifikującym jest wyrządzenie przez sprawcę znacznej szkody majątkowej.

W pierwszej części przepisu art. 268a § 1 k.k. dokonano kryminalizacji czynów, polegających na niszczeniu, modyfikacji danych i utrudnianiu do nich dostępu. Natomiast w drugiej – działań polegających na istotnym zakłócaniu (czyli utrudnianiu funkcjonowania systemu informatycznego) lub uniemożliwianiu przetwarzania, gromadzenia lub przekazywania danych informatycznych. Sformułowanie to odnosi się do wszelkich czynności oddziałujących na

2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tj. Dz.U. z 2016 r., poz. 1897 ze zm.).

32 W świetle przepisu art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2017 r., poz. 570 ze zm.), dalej jako ustawa o informatyzacji, jest to „materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej" – w zakresie tego pojęcia mieszczą się w nim wszystkie nośniki danych, czyli: niespotykane obecnie dyskietki, dyski twarde (nośniki magnetyczne), płyty CD i DVD (nośniki optyczne), pamięci półprzewodnikowe (są to m.in. pamięci RAM – *Random Access Memory*, ROM – *Read Only Memory*, jak również pamięci zamontowane, np. w drukarkach), pamięci *flash* itd.

33 Tak też: A. Adamski, *Prawo karne...*, s. 64–65.

34 P. Kardas, *Prawnokarna ochrona…*, s. 88.

35 Ibidem. Zob. także: P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks…*, s. 621; W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1296.

36 O. Górniok [w:] O. Górniok i in., *Kodeks karny. Komentarz*, t. 2, Gdańsk 2005, s. 363–364; M. Kalitowski [w:] M. Filar (red.), *Kodeks karny. Komentarz*, Warszawa 2012, s. 1209.

te procesy, których skutkiem jest ich nieprawidłowy przebieg lub spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych danych informatycznych[37].

Omawiany czyn ma swój typ kwalifikowany określony w art. 268a § 2 k.k. Znamieniem kwalifikującym jest spowodowanie przez sprawcę znacznej szkody majątkowej.

Istotą przestępstwa tzw. sabotażu informatycznego określonego art. 269 § 1 k.k. jest niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Zgodnie z przepisem art. 269 § 2 k.k. przestępstwo sabotażu informatycznego polegać może również na niszczeniu albo wymianie informatycznego nośnika danych lub niszczeniu albo uszkadzaniu urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania chronionych danych informatycznych. Zagrożone jest ono wysoką sankcją – karą pozbawienia wolności od sześciu miesięcy do ośmiu lat.

Z uwagi na znacznie wyższe znaczenie informacji chronionych przez przepis art. 269 § 1 k.k. w porównaniu z informacją podlegającą ochronie na podstawie art. 268 § 2 k.k. oraz identyczność pozostałych znamion czynów kryminalizowanych przez te przepisy, przy jednoczesnej różnicy w wysokości zagrożenia karą i środkami karnymi, przestępstwo z art. 269 § 1 k.k. uważa się za typ kwalifikowany w stosunku do przestępstwa z art. 268 § 2 k.k.[38] Z tych też względów twierdzenie takie jest moim zdaniem uzasadnione również w przypadku stosunku między przestępstwami z art. 268a k.k. lub 269a a 269 § 1 k.k.

Przepis art. 269a k.k. przewiduje odpowiedzialność karną osoby, która bez uprawnienia w stopniu istotnym zakłóca pracę systemu informatycznego,

37 W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1520.

38 P. Kardas, *Prawnokarna ochrona…*, s. 96. Tak też: A. Adamski, *Prawo karne…*, s. 77; M. Kalitowski [w:] M. Filar (red.), *Kodeks…*, s. 1211.

systemu teleinformatycznego[39] lub sieci teleinformatycznej[40] poprzez działania o charakterze logicznym, takie jak transmisja, zniszczenie, uszkodzenie lub zmiana danych informatycznych. Przedmiotem ochrony jest bezpieczeństwo pracy systemu komputerowego, a co za tym idzie – dostępność przetwarzanych w nim danych informatycznych.

Zamach na pracę systemu informatycznego, teleinformatycznego i sieci teleinformatycznej jest zamachem logicznym, a nie fizycznym – zakłócenie ma być wywołane przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych. Będą to np. ataki typu DoS.

Andrzej Adamski[41] i Włodzimierz Wróbel[42] zauważają, że przepisy art. 268a i 269a k.k. nakładają się na siebie zakresowo. Określenia „w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie danych" oraz „w istotnym stopniu zakłóca pracę systemu informatycznego, teleinformatycznego i sieci teleinformatycznej" są w istocie tożsame. Praca ww. systemów oraz sieci teleinformatycznej polega właśnie na przetwarzaniu, gromadzeniu i przekazywaniu danych. A. Adamski proponuje, by przepis art. 268a k.k. traktować jako narzędzie służące ściganiu sprawców, któ-

39 Stosownie do art. 2 pkt 3 ustawy o informatyzacji, jest to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu prawa telekomunikacyjnego (identyczna definicja znajduje się w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2016 r., poz. 1030 ze zm.). Przyjmuje się, że system informatyczny służy przetwarzaniu danych, natomiast system telekomunikacyjny przesyłaniu tych danych. Stąd system teleinformatyczny jest systemem informatycznym (w którym dane komputerowe są przetwarzane) podłączonym do sieci telekomunikacyjnej, za pośrednictwem której może wysyłać i odbierać dane. Por. X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 62–64; F. Radoniewicz, *Odpowiedzialność karna…*, s. 282–284.

40 Pojęcie to nie jest obecnie zdefiniowane w żadnym akcie prawnym. Sieć teleinformatyczna jest zespołem systemów teleinformatycznych, czyli systemów informatycznych, w których przetwarzane są dane, powiązanych ze sobą sieciami telekomunikacyjnymi, służącymi przesyłaniu danych między tymi systemami. Jest to struktura rozległa, której powstanie związane jest z procesem konwergencji technologii informatycznej i telekomunikacji. Por. X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 62–64; F. Radoniewicz, *Odpowiedzialność karna…*, s. 284; M. Świerczyński [w:] J. Gołaczyński, K. Kowalik-Bańczyk, A. Majchrowska, M. Świerczyński, *Komentarz do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*, Warszawa 2009, s. 39; A. Urbanek [w:] J. Chustecki i in., *Vademecum teleinformatyka*, Warszawa 1999, s. 4–5.

41 A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4, s. 58–59.

42 W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1527.

rych zachowania nie wypełniły znamion strony przedmiotowej art. 269a k.k.[43] W. Wróbel natomiast postuluje stosować przepis art. 269a k.k. wówczas, gdy następuje kwalifikowane zakłócenie pracy systemu lub sieci[44]. Za typ kwalifikowany czynu z art. 269 a k.k. należy uznać przestępstwo z art. 269 § 1 k.k.

Podobnie jak w przypadku czynu z art. 267 § 2 k.k. zastosowanie znaleźć może instytucja z art. 269c k.k.

W artykule 269b k.k. spenalizowano czyny zabronione, których przedmiotem wykonawczym są „narzędzia hackerskie". Przepis art. 269b § 1 k.k., będący odpowiednikiem art. 7 dyrektywy 2013/40, kryminalizuje wytwarzanie, pozyskiwanie, zbywanie, udostępnianie: 1) urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4 k.k. (sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach), a także w art. 267 § 3, art. 268a § 1 albo 268 a § 2 w zw. z 268a § 1, art. 269 § 1 lub 2 albo art. 269a k.k.; 2) haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub w sieci teleinformatycznej.

Rozwiązania przyjęte w przepisie art. 269b § 1 k.k. od momentu wprowadzenia go do Kodeksu karnego nowelizacją z 2004 r. powszechnie krytykowane. Przede wszystkim wskazywano na brak klauzuli wyłączającej odpowiedzialność karną administratorów i osób zajmujących się bezpieczeństwem systemów informatycznych, którzy używają tego typu programów w procesie tworzenia zabezpieczeń systemów oraz ich testowania czy twórców oprogramowania antywirusowego[45]. Tę wadę wprawdzie w zasadzie usuwa ostatnia nowelizacja[46], ale pozostawia ona inne „niedociągnięcia". Wśród

43 A. Adamski, *Cyberprzestępczość…*, s. 58.

44 W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1527.

45 P. Gienas, *Uwagi do przestępstwa stypizowanego w art. 269b kodeksu karnego*, „Prokurator" 2005, nr 1, s. 82; F. Radoniewicz, *Odpowiedzialność karna…*, s. 336. Por. W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1530.

46 Do art. 269b dodano bowiem § 1a w brzmieniu: „Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia". Jednocześnie podwyższono górną granicę kary grożącej za to przestępstwo do 5 lat pozbawienia wolności, co uzasadniono jedynie koniecznością umożliwienia zastosowania wobec sprawcy tego czynu instytucji tzw. przepadku rozszerzonego, przewidzianego w art. 45 § 2 k.k. (Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, druk nr 1186, pkt 4.6). Spotkało się to ze słuszną krytyką (O (braku) odpowiedzialności karnej za szukanie luk w systemach i sieciach informatycznych – opinia

nich – w pierwszej kolejności – zwrócić należy uwagę na brak w zawartym w treści art. 269b § 1 k.k. katalogu przestępstw (do których popełnienia wytwarzanie, pozyskiwanie, zbywanie, udostępnianie urządzeń i programów jest kryminalizowane), wskazania hackingu, zarówno w postaci nieuprawnionego uzyskania informacji z art. 267 § 1 k.k., jak i nieuprawnionego dostępu do systemu informatycznego z art. 267 § 2 k.k.[47]

Co się tyczy innych mankamentów przepisu art. 269b § 1 k.k.– przede wszystkim mowa w nim o programach „przystosowanych" do popełnienia określonych w nim czynów. Istnieje zatem problem, jak ocenić działanie twórcy programu spełniającego kilka funkcji (chodzi o tzw. programy o podwójnej naturze)[48], użytego następnie przez osobę trzecią w celach przestępczych, czego autor by sobie nie życzył[49]. W celu zachowania *ratio legis* wprowadzenia tego przepisu i uniknięcia zbyt szerokiej kryminalizacji W. Wróbel zaproponował jego interpretację nawiązującą do definicji karalnych czynności przygotowawczych z art. 16 § 1 k.k., wymagając tym samym od sprawcy wytwarzającego lub pozyskującego wymienione w przepisie narzędzia, zamiaru bezpośredniego (w przypadku zbywania i udostępnianiu poprzestając na wymogu zamiaru ewentualnego)[50]. Jak się jednak wydaje, większość przedstawicieli doktryny uważa jednak (z wyjątkiem – właśnie W. Wróbla i Joanny Piórkowskiej-Flieger, Barbary Kunickiej-Michalskiej[51] i Andrzeja

prawna Fundacji Frank Bold i Krakowskiego Instytutu Prawa Karnego, http://blog.frankbold.pl/bug-bounty/).

47 Brak w katalogu przestępstwa z art. 268 § 2 k.k. jest mniej problematyczny – do popełnienia czynu w nim określonego będą służyć te same programy, co w przypadku czynów z art. 268a § 1 i 2 k.k. oraz art. 165 § 1 pkt 4 k.k. (np. wirusy).

48 Np. monitory sieciowe, inaczej nazywane analizatorami protokołów, umożliwiające administratorom analizę ruchu w sieci, mogą zostać wykorzystane przez hackerów jako *sniffery*.

49 Por. A. Adamski, *Cyberprzestępczość…*, s. 60.

50 W. Wróbel [w:] A. Zoll (red.), *Kodeks…*, s. 1529–1530. Podobnie J. Piórkowska-Flieger [w:] T. Bojarski (red.), *Kodeks karny. Komentarz*, Warszawa 2012, s. 713.

51 B. Kunicka-Michalska uważa, że trudno wyobrazić sobie wytwarzanie, pozyskiwanie czy zbywanie bez zamiaru bezpośredniego sprawcy; zob. B. Kunicka-Michalska [w:] A. Wąsek, R. Zawłocki (red.), *Kodeks karny. Część szczególna. Komentarz. Komentarz do artykułów 222–316*, t. II, Warszawa 2010, s. 748.

Marka[52]), że dla przypisania sprawcy winy wystarczy, by działał on w zamiarze ewentualnym[53].

Zakończenie

Polska regulacja przestępstw komputerowych wymaga niewątpliwie zmian. W pierwszej kolejności należy ujednolicić siatkę pojęciową. Obecnie – z uwagi na ratyfikację Konwencji o cyberprzestępczości – nie zachodzi już konieczność definiowania pojęcia danych informatycznych (komputerowych), gdyż zawarta w niej definicja ma charakter normy samowykonywalnej i może być bezpośrednio stosowana. Z uwagi na omówione szeroko wątpliwości dotyczące zakresu pojęć „system informatyczny" należałoby je zdefiniować. Podobnie należy uczynić w przypadku terminu „sieć teleinformatyczna". Ewentualnie można rozważyć zastąpienie go pojęciem „sieć telekomunikacyjna".

Uważam, że należy przemyśleć ograniczenie zakresu kryminalizacji przepisu art. 267 § 1 k.k. do przypadków naruszenia tajemnicy korespondencji, przy jednoczesnym przyznaniu głównej roli w walce z *hackingiem* (uzyskania nieuprawnionego dostępu do systemu informatycznego) przepisowi art. 267 § 2 k.k., po uzupełnieniu go o wymóg, by sprawca zniwelował lub ominął magnetyczne, elektroniczne, informatyczne lub inne szczególne zabezpieczenie

52 Według A. Marka czynności sprawcze wymienione w przepisie art. 269b § 1 k.k. mogą być popełnione jedynie w zamiarze bezpośrednim, zaś zamiarem ewentualnym może być objęte przeznaczenie urządzeń, programów, haseł, kodów dostępu i innych danych; zob. A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, s. 576. J.W. Giezek, krytycznie odnosząc się do stanowiska, iż wytwarzania i pozyskiwania dopuścić się można jedynie w zamiarze bezpośrednim, podkreśla wręcz, iż bardziej prawdopodobne wydaje się popełnienie tego przestępstwa w zamiarze ewentualnym, gdy sprawca jedynie godzi się na to, że swoim zachowaniem wypełni znamiona przestępstwa, gdyż zwykle sytuacja będzie przedstawiać się w ten sposób, iż nie tyle chce wytworzyć, pozyskać, zbyć lub udostępnić określone urządzenia lub programy komputerowe, lecz że z pewnym jedynie prawdopodobieństwem zakłada, że okażą się one przystosowane do popełnienia jednego z określonych w komentowanym przepisie przestępstw, godząc się, że tak właśnie będzie. Autor ten sugeruje wręcz, że owa „niepewność diagnozy" np. co do przystosowania urządzeń lub programów pozwala przyjąć, że mamy w takim przypadku do czynienia jedynie z zamiarem ewentualnym , J.W. Giezek [w:] J.W. Giezek (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014, s. 1007–1008.

53 Zob. np.: A. Adamski, *Cyberprzestępczość…*, s. 61; K. Gienas, *Uwagi do przestępstwa…*, s. 81–82; O. Górniok [w:] O. Górniok i in., *Kodeks…*, s. 369–370; M. Kalitowski [w:] M. Filar (red.), *Kodeks…*, s. 1214; P. Kozłowska-Kalisz [w:] M. Mozgawa (red.), *Kodeks…*, s. 629.

(jednocześnie byłoby to zgodne z postanowieniami art. 3 dyrektywy 2013/40, która zaleca takie rozwiązanie[54]).

Konieczna jest modyfikacja polskiej regulacji podsłuchu komputerowego. Artykuł 267 § 3 k.k. wymaga bowiem wystąpienia po stronie sprawcy zamiaru kierunkowego, a przesłanki takiej nie przewiduje art. 6 dyrektywy 2013/40. Ewentualnie rozważyć można pozostawienie go w dotychczasowym (lub zbliżonym) brzmieniu, przy jednoczesnym dodaniu przepisu (zgodnego z art. 6 dyrektywy 2013/40), określającego czyn, w stosunku do którego występek z obecnego art. 267 § 3 k.k. stanowiłby typ kwalifikowany.

Zmian w również wymaga przepis art. 269b § 1 k.k. Konieczne jest ograniczenie odpowiedzialności do zamiaru bezpośredniego oraz wskazanie, że dotyczy on narzędzi i programów komputerowych „przede wszystkim" lub „głównie" (w angielskim tekście dyrektywy 2013/40 użyto pojęcia *„primarily"* tekście, w polskim – właśnie „głównie") służącym popełnieniu przestępstw. Ponadto należy rozszerzyć katalog przestępstw, do których popełnienia miałyby one służyć co najmniej o pozostałe omawiane czyny.

Bibliografia

Literatura

Clifford R.D. (red.), *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime*, Durham 2011.

Adamski A., *Botnety jako zagadnienie prawno-kryminologiczne na tle doświadczeń amerykańskich*, „Prokuratura i Prawo" 2013, nr 1.

Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4.

Adamski A., *Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?*, „Prawo Teleinformatyczne" 2007, nr 3.

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Bojarski T. (red.), *Kodeks karny. Komentarz*, Warszawa 2012.

Bukowski S., *Przestępstwo hackingu*, „Przegląd Sądowy" 2006, nr 4.

Clough J., *Principles of Cybercrime*, New York 2013.

Czechowski R., Sienkiewicz P., *Przestępcze oblicza komputerów*, Warszawa 1993.

Dudka K., *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin 1998.

Filar M. (red.), *Kodeks karny. Komentarz*, Warszawa 2012.

Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000.

Gienas P., *Uwagi do przestępstwa stypizowanego w art. 269b kodeksu karnego*, „Prokurator" 2005, nr 1.

Giezek J.W. (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014.

54 „Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor". Zob. także: F. Radoniewicz, *Odpowiedzialność karna…*, s. 459.

Gołaczyński J., Kowalik-Bańczyk K., Majchrowska A., Świerczyński M., *Komentarz do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*, Warszawa 2009.
Grabosky P., *Electronic Crime*, New Jersey 2006.
Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.
Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004.
Koops B.J., Robinson T., *Cybercrime Law: A European Perspective* [w:] E. Casey (red.), *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, Waltham–San Diego–London 2011.
Krasuski A., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010.
Marek A., *Kodeks karny. Komentarz*, Warszawa 2010.
Mozgawa M. (red.), *Kodeks karny. Praktyczny komentarz*, Warszawa 2012.
Piątek S., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko komputerowym i systemom informatycznym*, Warszawa 2016.
Shinder D.L., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004.
Sieber U., *Legal Aspects of Computer-Related Crime in the Information Society – Comcrime – Study*, Würzburg 1998.
Siwicki M., *Definicje i podział cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.
Smarzewski M., *Cyberprzestępczość a zmiany w polskim prawie karnym* [w:] I. Sepioło-Jankowska (red.), *Reforma prawa karnego. Księga po Zjeździe Młodych Karnistów*, Warszawa 2014.
Wall D., *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013.
Wąsek A., Zawłocki R. (red.), *Kodeks karny. Część szczególna. Komentarz. Komentarz do artykułów 222–316*, t. II, Warszawa 2010.
Wójcik J.W., *Przestępstwa komputerowe. Fenomen cywilizacji*, cz. I, Warszawa 1999.
Zoll A. (red.), *Kodeks karny. Komentarz. Część szczególna. Komentarz do artykułów 117–277 k.k.*, t. II, Warszawa 2013.

Akty prawne

Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 69, s. 67).
Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218, s. 8).
Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w prawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz.Urz. UE L 127, s. 39).
Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).
Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczącego penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych z dnia 28 stycznia 2003 r. (Dz.U. z 2015 r., poz. 730).
Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2016 r., poz. 1489 ze zm.).
Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2017 r., poz. 570 ze zm.).
Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tj. Dz.U. z 2016 r., poz. 1897 ze zm.).
Ustawa z dnia 6 kwietnia 1990 r. o Policji (tj. Dz.U. z 2016 r., poz. 1782 ze zm.).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2016 r., poz. 1137 ze zm.).

Computer crimes in the Polish Penal Code

Abstract

The aim of the paper is to analyze the provisions criminalizing the phenomenon of "computer crimes" ("cyber crimes") in the strict sense, ie acts in which a computer or network is the target of a crime ("a victim"). The paper consists of three parts – a short introduction in which the most important terminological issues are discussed in a synthetic way, the main part in which analisis of articles 267–269c of the Penal Code of 1997 (Chapter XXXIII, entitled "Offenses against the protection of information" – in which the Polish legislator defined these offenses – is carried out. The last part is the summary containing comments de legelata and de lege ferenda.

Key words: cybercime, hacking, hackingtools, surveillance, data interception

Katarzyna Badźmirowska-Masłowska*

Child protection in cyberspace

Abstract

The aim of this article is to review main issues connected with the protection of a child in the cyberspace. It indicates the issue of the scientific discourse within the key terms: cyberspace and security of an underage in the online and offline environment. In the context of his position as mass media recipient and an user of cyberspace, several threats have been indicated and allocated to two basic categories: of macro-social and individual character. Premises shaping the systems of child's security in the cyberspace have been indicated and the use of legal instruments and alternative methods in terms of specific security threats has been noted. Ultimately, current challenges to increase the effectiveness of providing security in the cyberspace for an underage were formulated.

Key words: security, protection, child, underage, threat, the media

* Dr Katarzyna Badźmirowska-Masłowska, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: k.badzmirowskam@gmail.com.

Introduction

Child protection[1] in cyberspace, understood in the informative context of its kind[2], is a complex subject of consideration of almost all fields and many scientific disciplines[3], setting the framework for systemic (ergo containing complementary instruments of hard and soft law and alternative measures) protection of a juvenile. This implies a number of controversies, in particular, regarding fundamental terminological issues, i.e. a child or cyberspace, i.e. the subject and the ecosystem of its daily functioning.

The very definition of "a child", traditionally meaning in the context of Article 1 of the Convention on the Rights of the Child of November 11, 1989[4] any human being under 18 years of age is not precise enough to properly address the subject issues. First of all, for the audio-visual sector, and more broadly - the space determined by the development of information and communication technologies (ICT), "a child" is determined both at the international/ supranational level, covering in its scope various categories of children and young people (referred to as *a child*, *children*, *minors*, *adolescents*, *youth*, *young people*); at the national level, on the other hand, more detailed solutions are provided from the point of view of protecting safety of individual age groups against standardized types of threats, taking into account internal regulations defining the concepts of a minor, an underage or a juvenile and an adolescent. It is also necessary to take into account different - and determined in a simplified way – passive status of the recipient in linear audio-visual services and the user in the online environment[5], determining the roles a child can fulfil- a participant presenting specific behaviours, an actor (player), shaping interpersonal

1 Pojęcia dziecko i małoletni używa się w tej pracy zamiennie.

2 Por. K. Badźmirowska-Masłowska, *Małoletni użytkownik internetu a zagrożenia bezpieczeństwa informacji* [w:] W. Kitler, J. Taczkowska (red.), *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, Warszawa 2017, s. 318–333.

3 Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r., w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. z 2018 r., poz. 1818).

4 Konwencja o prawach dziecka z dnia 20 listopada 1989 r. (Dz.U. z 1991 r. nr 120, poz. 526).

5 Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) (Dz.Urz. UE L95, s. 1); por. też rewizję dyrektywy z dnia 6 listopada 2018 r.

relations and contents creator, even if it violates the regulations of the law, including criminal law or becoming a victim (an injured or harmed person). It should also be emphasized that the picture of threats should be perceived more broadly and in a more diverse way than in the case of adults, which is due to the fact that the subject of protection in the ecosystem in question is not a child in se, but the regularity of its psychophysical, socio-cultural and moral development. Furthermore, it means that child's social maladjustment should also be analysed in this respect.

Child's protection in cyberspace. Dilemmas with definitions

The concept of cyberspace which is derived from the classic novel of cyberpunk – as a variation of science fiction[6], although widely accepted in the language of the law and the lawyers, not only has it not been unequivocally accepted at the international/ supranational[7] or national level[8] of the legal definitions, but it is not sufficient for considerations regarding the safety of the juvenile

6 Por. W. Gibson, Neuromancer, P.W. Cholewa (tłum.), *Książnica*, Katowice 2009, s. 59; notabene odwołuje się ono do cybernetycznych koncepcji łączenia świata zwierzęcego (ludzkiego) i maszyn, N. Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine*, Nowy Jork 1948.

7 Najwięcej wątpliwości pojawia się wokół kwestii związanych z regulacją i jurysdykcją sfery internetowej. Na forum międzynarodowym i w poszczególnych państwach toczą się debaty nad zagadnieniami związanymi z implikacjami politycznymi, ekonomicznymi oraz społeczno-kulturowymi jej rozwoju w kontekście potrzeby, ale też i możliwości efektywnej jej regulacji, w szczególności odnoszącej się do zawartości. Kwestia ta budzi kontrowersje nie tylko na europejskim poziomie regionalnym, ale także w perspektywie globalnej (por. kontrowersje wokół Communications Decency Act, np. R. Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, „Law Journal" 1996, nr 1, s. 51–59). Z jednej strony podtrzymywane są zatem koncepcje stojące u podstaw charakterystyki ogólnoświatowej sieci jako teoretycznie nieinwigilowanej przestrzeni przepływu informacji i zawiadywanej dotychczas przez The Internet Corporation for Assigned Names and Numbers (ICANN – por. E. Salomon, K. Pijl, Applications to ICANN for Community based New Generic Top Level Domains (gTLDs): Opportunities and challenges from ahuman rights perspective, Council of Europe report, DGI(2016)17), z drugiej zaś obserwuje się inicjatywy na rzecz objęcia internetu międzynarodowymi i krajowymi regulacjami prawnymi, co z kolei budzi obawy przed jego upolitycznieniem i poddaniem pod zarząd International Telecommunication Union (ITU). RE iUE prezentują stanowisko pośrednie, np. M. Kenig-Witkowska, *Niektóre zagadnienia prawno-międzynarodowej regulacji Internetu*, „Państwo i Prawo" 2001, z. 9, s. 58 i nast.; por. też uwagi ITU (Internet Policy and Governance), online.

8 Por. definicję odpowiadającą zasadniczo technologicznemu punktowi widzenia, zawartą w ustawie z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz

in the overlapping dimensions of offline and online life[9]; the technological, information and political and economic perspectives should be supplemented by the socio-cultural aspects of the virtual communication[10], which is not unreal, although existing in experience detached from direct and creating other forms of socialization[11]. The new cultural paradigm is embedded in an approach sometimes opposing the technological determinism of the constructivist concept[12], while it seems more justified to consider the network formula as part of technology of its incorporation into the everyday lives of individuals and society rather than being separate and parallel to reality[13]; virtual reality is a process through which the information society expresses itself[14] .

o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. nr 222, poz. 1323).

9 W zmediatyzowanych społeczeństwach zacierają się granice między rzeczywistym życiem a jego wirtualnym obrazem; S. Lash, J. Urry, *Postmodernist Sensibility* [w:] A. Giddens, D. Held, S. Loyal, D. Seymour, J. Thompson (red.), *The Polity Reader in Cultural Theory*, Cambridge 1994, s. 135. Wobec potrzeby łącznego postrzegania rzeczywistości realnej i wirtualnej dyskusje dotyczą też koncepcji autonomizacji cyberkultury prawnej, por. K. Dobrzeniecki, *Autonomiczne prawo cyberprzestrzeni: mit czy rzeczywistość?* [w:] O. Bogucki, S. Czepita (red.), *System prawny a porządek prawny*, Szczecin 2008, s. 316 i nast.; J. Janowski, *Globalna cyberkultura polityki i prawa* [w:] M. Maciejewski, M. Marszał, M. Sadowski (red.), *Tendencje rozwojowe myśli politycznej i prawnej*, Wrocław 2014, s. 311–325.

10 Por. D. de Kerckhove, *Inteligencja otwarta. Narodziny społeczeństwa sieciowego*, online; M. Szpunar, *Przestrzeń internetu – nowy wymiar przestrzeni społecznej* [w:] A. Siwik, I. Haber (red.), *Od robotnika do internauty. W kierunku społeczeństwa informacyjnego*, Kraków 2008, s. 225–234 (i cytowana tam literatura). Przy czym niezasadne jest ani zbyt wąskie utożsamianie cyberprzestrzeni z technologicznym pojęciem internetu, ani z nadmiernie upraszczającą synonimizacją jej ze sferą wirtualną, J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 57; M. Ostrowicki, *Wirtualne realis. Estetyka w epoce elektroniki*, Kraków 2006, s. 119 i nast.

11 Należy rozważyć, że w istocie rzeczywistość, której człowiek doświadcza, jest zawsze wirtualna, bowiem postrzegana jest właśnie przez symbole, K. Krzysztofek, *Zmiana permanentna? Refleksje o zmianie społecznej w epoce technologii cyfrowych*, „Studia Socjologiczne" 2012, nr 4, s. 9.

12 Por. np.: M. Szpunar, *Nowe-stare medium. Internet między tworzeniem nowych modeli komunikacyjnych a reprodukowaniem schematów komunikowania masowego*, Warszawa 2012, pkt 1.4, *Konstruktywizm versus technologiczny determinizm*, s. 33–44.

13 Por. np.: M. Castells, *Społeczeństwo sieci*, M. Marody, K. Pawluś, J. Stawiński, S. Szymański (tłum.), Warszawa 2010, s. 46–47; T. Goban-Klas, *Społeczeństwo medialne*, Warszawa 2005, s. 165 i nast.; M. Gruchoła, *Nowe formy zachowań społecznych wobec i pod wpływem mediów oraz nowych technologii. Analizy porównawcze*, „Państwo i Społeczeństwo" 2017, nr 3, s. 12 i nast.

14 R.W. Kluszczyński, *Społeczeństwo informacyjne. Cyberkultura. Sztuka multimediów*, Kraków 2001, s. 80; Globalne Społeczeństwo Informacyjne (GSI) za: P. Sienkiewicz, H. Świeboda, *Ewaluacja strategii rozwoju społeczeństwa informacyjnego*, „Zeszyty Naukowe. Ekonomiczne Problemy Usług" 2010, nr 57; *E-gospodarka w Polsce. Stan obecny i perspektywy rozwoju*,

The impact of ICT is most strongly observed in the category of a juvenile, for whom they become an integral and important part of life, *ergo* the intensity of social change is associated here with particular vulnerability to their impact, especially in the conditions of replacement of national and regional cultures with global patterns; especially since contemporary, individual mass media are now entering the area traditionally affected by primary structures, such as family, school, and friends. To consider the title issues, the concept of cyberspace, adopted in the legal regulations, doctrine and jurisprudence, needs to be supplemented with the perspective of other scientific disciplines dealing with communication issues (science of social communication and media, sociology, psychology, pedagogy, security science, but also linguistics, philosophy, telecommunications)[15].

In the light of the revolutionary pace of changes in the overall life of modern societies and individuals creating them, caused by the rapid development of ICT, the perception of the safety of a juvenile in the information and its social context also undergoes transformation. Apart from the need to use broader than negative approaches to security, it is crucial to categorize threats (*risks*, *dangers*, *threats*) in the paradigm of macro-social preponderance or an individual perspective of their consideration[16].

In the first category, attention deserve the following negative effects: 1) digital exclusion; 2) global, uniformed cultural patterns, often in opposition to the axiological systems of communities traditionally adopted in a given region; 3) concentration around consumer and mercantile values, changing especially the concepts of privacy and security in the economic area.

In the second category, however: 1) sexual crime against a child; 2) the content traditionally considered harmful to the development of a juvenile recipient (pornography and violence); 3) technologically implied transformations of traditional threats (cyberthreats), deciding on their

cz. I, Szczecin 2010, s. 132; P. Sienkiewicz, *Teoria rozwoju społeczeństwa informacyjnego* [w:] L.H. Haber (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, Kraków 2002, s. 506–507.

15 Zagadnienie wymaga szerszego, odrębnego opracowania; tu wskazano jedynie główne aspekty podlegające dyskusji.

16 Por. K. Badźmirowska-Masłowska, *Zagrożenia dla małoletniego ze strony mediów audiowizualnych. W kierunku nowego paradygmatu?* [w:] M. Szymczyk, R. Grzywacz (red.), *W trosce o człowieka. Paradygmaty stare i nowe*, Kraków 2016, s. 239–250.

intensity and increase in the scope (e.g. *cyberbullying*); 4) hazards specific to online environment (e.g. addictions).

The threats in question affect the following sphere: sexual (erotic), aggression, values, and relate both to the status of the child as a recipient of mass media, as well as the participant, actor and creator of their network types. Despite the fact that the juvenile comes into contact with a wide spectrum of these dangers, one should bear in mind that the very risk of their occurrence does not mean automatic damage, but it is rather its probability that is estimated, especially since the network ecosystem creates a kind of a dual space called risky opportunities, on the one hand conducive to the child's development, and on the other, exposing the child to unprecedented dangers[17]. Vulnerability of a juveniles shaped at the macro-social and individual level, in a way in opposition to the ability to deal effectively with them, to respond to them in a balanced way (*resilience*) and to constructively cope with them (*cope*), determined by their awareness, psychophysical fitness and social, knowledge and skills, *ergo* media competence[18]; the individual paradigm created by the above conditions the adopted methods of protecting a minor in cyberspace.

Methods of protecting a juvenile in cyberspace

The purpose of protecting a child in cyberspace is, on the one hand, to ensure the child's safety and, on the other, to ensure proper conditions of the child's development. Referring to the aspect of counteracting threats, nota bene, usually perceived analogically to the offline sphere and in accordance with the principle of technological neutrality[19], one should indicate the need for its systemic shaping, based on its *multi-layered*, encompassing many stakeholders and multi-level (*multi-level*) approach[20].

17 18 Por. np. recommendation of the OECD The protection of children online, 2012; OECD Council report on risks faced by children online and policies to protect them, 2012, online, szerzej, por. np.: K. Badźmirowska-Masłowska, *Protecting minors from internet threats. Legal instruments or alternative measures?* [w:] M. Sitek, A.F. Uricchio, I. Florek (red.), *Human Rigts, between needs and possibilities*, Józefów 2017, s. 35–58 (i cytowana tam literatura).

18 Ibidem.

19 Por. np.: N. van Eijk, *Net Neutrality and Audiovisual Services*, „Iris plus" 2011, nr 5, s. 7–19.

20 OECD Report on risks faced by children online and policies to protect them has indicated the various dimensions of child protection policy: multi-layered, multi-stakeholder and multi-level..., s. 40–49.

The first component contains direct and indirect tools that combine legal instruments with alternative methods.

The category of the stakeholders covers a wide range of obligation sharing recipients, from the representatives of public authorities (especially relevant ministers of education, culture, health, justice, etc.), the representatives of business (media, telecommunications, etc.) to the information society (civil, e.g. in the form of NGOs); special attention should be given to parents/guardians, school or broadly understood educational environment.

What is important, it is indicated that the objectives of the protection in question should be adopted, within the framework of regional standards (here European), at the governmental level, which allows monitoring their implementation, proposing new initiatives, establishing and conducting cooperation within national and international (transnational) and finally promotes cooperation between the private (commercial) and non-governmental sectors. Multilevel politics means conducting it both at the state level and - on the basis of cooperation – at the international level, while in the case of the European continent both the Council of Europe and the European Union constitute in this respect regional standards of soft or hard law, depending on the type of threat. Harmonization of regulations and cooperation within programs, due to the cross-border nature of cyberspace, is a necessary condition for the effectiveness of national security systems.

When considering the basic premises for choosing legal or alternative methods of protecting a minor, the following should be indicated: 1) seriousness of the threat – constituting a crime or other disruption to the correct development of the child, with sexual offenses directed against him defined as particularly harmful[21]; 2) technical aspects of access to dangerous content, contacts and behaviour – depending on the type of audio-visual service (linear or on demand) or other service provided by the internet (especially individual mass media); 3) extent of a given threat – determining both the macro-social or individual nature of it and the need for an internal or international level of response; 4) the age category of children and youth- setting protection measures appropriate to the minor's development level (both in technical and social terms). According to the aforementioned premises, different types of legal

21 Overall, legislation pertaining to all illegal content is applying across all offline and online media and it is predominantly regulated on national level within the scope of general laws (e.g. consumer or privacy and information security related risks for minors), K. Badźmirowska-Masłowska, *Protecting*..., s. 45.

instruments and alternative measures are applied to the identified types of threats. In general[22], criminal law instruments are mainly used in the area of sexual crime against the child[23]; they specify which deeds should be criminalised, the amount of the minimum maximum penalties and raise the issue of the age of relevant consent to sexual activities. As regards procedural guarantees, the states are required to: ensure the conditions for reporting suspected sexual abuse or child sexual exploitation (art. 16 of Directive 2011/92/EU), assistance and support to minors who are the victims of crime before the commencement of preparatory proceedings, during its duration, as well as during legal proceedings (victims, art. 18–20 of the above-mentioned directives and Article 31–36 of the Lanzarote Convention). Furthermore, they should introduce preventive intervention programs or measures (art. 21–25 of the beforementioned directive and Article 4–17 of the Lanzarote convention).

Alternative methods are of particular importance to ensure child's protection in the online environment. In particular, the following are worth mentioning: 1) self and coregulation arising from the bottom up, as well as at the initiative of the regulating bodies[24]; 2) technical measures – restricting access, but also marking content[25]; 3) methods for strengthening awareness of threats – based on education or social (information) campaigns[26];

22 Szersze omówienie zagadnienia przekracza ramy tego opracowania.

23 Por. Konwencję Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, sporządzoną w Lanzarote dnia 25 października 2007 r., Dz.U. z 2015 r., poz. 608 oraz dyrektywę Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WsiSW, Dz.Urz. UE L 335, s. 1–14; szerzej, np.: K. Badźmirowska-Masłowska, *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective* [w:] M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (red.), *Europe of Founding Fathers. Investment in the Common future*, Olsztyn 2013, s. 147–160. Instrumenty prawne stosuje się także względem innych zagadnień, związanych np. z naruszeniami prywatności, por. np.: K. Badźmirowska-Masłowska, *Wizerunek dziecka w internecie a zagrożenia prawa do prywatności* [w:] K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak (red.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, s. 49–61.

24 Por. np. recommendation REC (2001)8 of the Committee of Ministers to member states on Self-regulation concerning cyber content.

25 Por. np. recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to internet filters.

26 Por. np. recommendation 1586 (2002) The digital divide and education; recommendation orazRec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment.

4) other – program-based assistance points, *so-called hot lines (helplines*, insafe, inhope)[27] or creating *child protection zones*[28].

Support may come from various stakeholder groups initiating actions at the national and international level for the implementation of children's rights[29]; the most well-known program here is Better Internet for Kids[30], and the research space – EU Kids Online[31].

Summary

When considering the issues of child protection in cyberspace, conclusions should be presented regarding initiatives and actions that should be raised to increase its effectiveness. The first issue is conducting extensive research in the field of: 1) terminological arrangements as to the concept of: 1) cyberspace – as an environment for the functioning of a minor, equal to offline reality, together with the determination of the interrelationship between both dimensions of its life; 2) the status of the child - as the recipient of audio-visual media and other audio-visual network services, in the context of being recognized as an object of protection for its proper development; 3) security – as an aspect of research on these issues; 2) changes in the role of audio-visual media, and more broadly the virtual / internet / cyberspace environment – as to the strength and scope of their impact on contemporary generations of children and youth.

The research above should be focused on creating a national strategy for the protection of a minor. It should be based on the pillars of the EU Safer Internet Strategy[32], which relates to: 1) publishing high-quality content (creative, educational) online for children and young people and promoting positive online experiences for children; 2) increasing awareness, especially

27 Online.
28 Np. online.
29 Global Alliance against Child Sexual Abuse Online, 2015 Threat AssesmentReoport, online.
30 Por. też: K. Badźmirowska-Masłowska, *Edukacyjne aspekty bezpieczeństwa nowych technologii komunikacyjnych dla małoletnich w świetle Strategii Unii Europejskiej na rzecz lepszego Internetu dla dzieci*, „Journal of Modern Science" 2012, nr 3, s. 433–472.
31 Online.
32 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia na rzecz lepszego internetu dla dzieci, COM(2012) 196 final.

of end users (parents / guardians, minors themselves etc.) and strengthening rights, shaping digital skills and using the media, including the introduction of online safety education in school programs and expanding information activities (e.g. campaigns) and enabling reporting of violations of law and security; 3) creating a safe online ecosystem for the juvenile by adapting privacy and advertising settings to age, popularizing the use of parental control tools, widespread use of age ratings and content classification; 4) combating sexual crime against a child in international cooperation through faster and systematic identification of materials depicting such acts. Both at the international (universal, regional, supranational) and national levels, a number of initiatives are observed focused on child protection in cyberspace and involving entities from the public, private and non-governmental sector. However, the analysis of the situation in Poland indicates that the already existing wide interaction of recipients of obligations, fulfilling the areas of prevention and combating undesirable effects, requires the development of appropriate procedures or mechanisms for coherent cooperation; therefore, the need to create a strategy for the protection of a minor in cyberspace, taking into account the penetration of offline and online worlds in everyday life as a fundamental premise, should be considered urgent. It should include legal instruments and alternative measures in a complementary manner, with particular emphasis on the issues of social education and systemic cooperation of stakeholders representing different categories; it should also resolve counteraction to which threats requires particularly intense cooperation at the international – regional/supranational or even universal level.

Bibliography

Literature

Badźmirowska-Masłowska K., *Edukacyjne aspekty bezpieczeństwa nowych technologii komunikacyjnych dla małoletnich w świetle Strategii Unii Europejskiej na rzecz lepszego Internetu dla dzieci*, „Journal of Modern Science" 2012, nr 3.

Badźmirowska-Masłowska K., *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective* [w:] M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (red.), *Europe of Founding Fathers. Investment in the Common future*, Olsztyn 2013.

Badźmirowska-Masłowska K., *Małoletni użytkownik internetu a zagrożenia bezpieczeństwa informacji* [w:] W. Kitler, J. Taczkowska (red.), *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, Warszawa 2017.

Badźmirowska-Masłowska K., *Protecting minors from internet threats. Legal instruments or alternative measures?* [w:] M. Sitek, A.F. Uricchio, I. Florek (red.), *Human Rigts, between needs and possibilities*, Józefów 2017.

Badźmirowska-Masłowska K., *Wizerunek dziecka w Internecie a zagrożenia prawa do prywatności* [w:] K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak (red.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017.
Badźmirowska-Masłowska K., *Zagrożenia dla małoletniego ze strony mediów audiowizualnych. W kierunku nowego paradygmatu?* [w:] M. Szymczyk, R. Grzywacz (red.), *W trosce o człowieka. Paradygmaty stare i nowe*, Kraków 2016.
Cannon R., *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, „Law Journal" 1996, nr 1.
Dobrzeniecki K., *Autonomiczne prawo cyberprzestrzeni: mit czy rzeczywistość?* [w:] O. Bogucki, S. Czepita (red.), *System prawny a porządek prawny*, Szczecin 2008.
Goban-Klas T., *Społeczeństwo medialne*, Warszawa 2005.
Gruchoła M., *Nowe formy zachowań społecznych wobec i pod wpływem mediów oraz nowych technologii. Analizy porównawcze*, „Państwo i Społeczeństwo" 2017, nr 3.
Janowski J., *Globalna cyberkultura polityki i prawa* [w:] M. Maciejewski, M. Marszał, M. Sadowski (red.), *Tendencje rozwojowe myśli politycznej i prawnej*, Wrocław 2014.
Kenig-Witkowska M., *Niektóre zagadnienia prawno-międzynarodowej regulacji Internetu*, „Państwo i Prawo" 2001, z. 9.
Kluszczyński R.W., *Społeczeństwo informacyjne. Cyberkultura. Sztuka multimediów*, Kraków 2001.
Krzysztofek K., *Zmiana permanentna? Refleksje o zmianie społecznej w epoce technologii cyfrowych*, „Studia Socjologiczne" 2012, nr 4.
Kulesza J., *Międzynarodowe prawo Internetu*, Poznań 2010.
Lash S., Urry J., *Postmodernist Sensibility* [w:] A. Giddens, D. Held, S. Loyal, D. Seymour, J. Thompson (red.), *The Polity Reader in Cultural Theory*, Cambridge 1994.
Ostrowicki M., *Wirtualne realis. Estetyka w epoce elektroniki*, Kraków 2006.
Sienkiewicz P., Świeboda H., *Ewaluacja strategii rozwoju społeczeństwa informacyjnego*, „Zeszyty Naukowe. Ekonomiczne Problemy Usług" 2010, nr 57.
Sienkiewicz P., *Teoria rozwoju społeczeństwa informacyjnego* [w:] L.H. Haber (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, Kraków 2002.
Szpunar M., *Nowe-stare medium. Internet między tworzeniem nowych modeli komunikacyjnych a reprodukowaniem schematów komunikowania masowego*, Warszawa 2012.
Szpunar M., *Przestrzeń internetu – nowy wymiar przestrzeni społecznej* [w:] A. Siwik, I. Haber (red.), *Od robotnika do internauty. W kierunku społeczeństwa informacyjnego*, Kraków 2008.
Wiener N., *Cybernetics: or Control and Communication in the Animal and the Machine*, Nowy Jork 1948.

Legal acts

Konwencja o prawach dziecka z dnia 20 listopada 1989 r. (Dz.U. z 1991 r. nr 120, poz. 526).
Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) (Dz.Urz. UE L95, s. 1).
Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. nr 222, poz. 1323).
Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r., w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. z 2018 r., poz. 1818).

Ochrona dziecka w cyberprzestrzeni

Streszczenie

Celem artykułu jest przegląd głównych zagadnień, łączących się z ochroną dziecka w cyberprzestrzeni. Wskazuje on na problematykę dyskursu naukowego w obrębie kluczowych pojęć, tj. cyberprzestrzeń i bezpieczeństwo małoletniego w środowisku *on-line* i *off-line*. W kontekście jego pozycji jako odbiorcy mass mediów i użytkownika cyberprzestrzeni, stypizowano poszczególne zagrożenia, przyporządkowując je dwóm podstawowym kategoriom: o charakterze makrospołecznym i indywidualnym. Wskazano na przesłanki kształtujące systemy ochrony dziecka w cyberprzestrzeni oraz zasygnalizowano stosowanie instrumentów prawnych i metod alternatywnych względem konkretnych zagrożeń. Finalnie sformułowano aktualne wyzwania dla zwiększenia efektywności zapewnienia małoletniemu bezpieczeństwa w cyberprzestrzeni.

Słowa kluczowe: bezpieczeństwo, ochrona, dziecko, małoletni, zagrożenie, media

Andrzej Pieczywok*

Cyber threats and challenges targeting man versus his education

Abstract

Modern man strongly emphasizes the need for security in all aspects of social and individual life. The content of the article concerns the threats and challenges for men in cyberspace. The author shows the relations and relationships between security and education. He devotes a lot of space to the characteristics of threats in cyberspace. Facing dynamically changing reality, the author makes the reader pay special attention to modern ways of counteracting threats generated from cyberspace. The article shows how broadly understood prevention and education in all possible stages of the human use of cyberspace are an important aspect of human life.

Key words: threats, challenges, education for safety, sense of security, human, society, prevention, teacher, the media, globalisation

* Dr hab. prof. nadzw. Andrzej Pieczywok, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, e-mail: a.pieczywok@wp.pl.

Introduction

We live in times that are extremely difficult to describe, define, and unambiguously incorporate into the existing paradigm of knowledge. It is even more difficult to identify universal social mechanisms and rules that will allow, even to a small extent, to predict actions, behaviors, processes or directions of social change. The saying "we live in a culture of acceleration and information revolution" already sounds like a cliché. The social reality of the early 21st century is a challenge for many of its researchers and observers.

It is worth noting that people today create society and culture largely through symbols, patterns and stories borrowed from the media coverage. This is how everyday reality is shaped and changed . Media recipients borrow ready-made patterns and behaviour patterns, and often also language expressions, which they transpose to the reality of everyday life. Thus, they create a global identity mediated through the media, global brands and companies, as well as marketing activities. The consequence of these phenomena is experiencing reality through the media coverage. Naturally, this is not the only way to receive and experience reality, but it certainly is a very important aspect of the modern existence and perception of the world by people.

People nowadays spend a lot of time consuming the media. Everyday life of ordinary people has never been so dominated by the "reality" learned through both the old media (television, radio, press, outdoor advertising) as well the new ones (global information and telecommunication network). Therefore, the paradox of the modern media is that as a result of the excess information taken out of context and as a result fascination with the extreme and the unique, people feel lost, and their actual, real knowledge of the world is getting poorer. Instead of increasing his knowledge of the world *and* events, a man loses orientation and ability to objectively assess facts.

The development of communication technologies, such as mobile communications and the internet, has caused major changes in the functioning of societies. It contributed to the creation of a new framework for the organization of human activities in individual, collective and global dimensions[1].

1 W przedmiocie nowych technologii komunikacyjnych i zagrożeń z nimi związanych zob. szerzej: K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015; M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa*

Computers streamline and make it easier for people to do any job, and the internet offers inexhaustible abundance of information on virtually any topic and connects people in a way that no other means of communication has ever provided. Thus, people with different levels of education and social status, often belonging to different cultures, using different languages, and attached to different religions can exchange thoughts and views with the help of the internet.

Broadly understood cyberspace[2] is not only a place where people work, gain knowledge, communicate with each other, and seek entertainment. It has also become a place where people are exposed to various threats.

Education is therefore one of the basic ways of developing security in cyberspace for humans and it affects their attitudes, values, messages and skills necessary to prevent threats, cope with emergencies and remove their effects. The conclusion is that it is through education, based however on a new paradigm, learning the ways and opportunities to acquire knowledge necessary for good functioning in a variable and risk-stressed reality is a way to a better knowledge and understanding of cyberspace.

Education can be defined as all processes that aim to change people, especially children and young people, according to the ideals and educational goals prevailing in a given society[3]. On the one hand, education is a factor in shaping human identity, and on the other, an indispensable creative condition for man's natural development. Depending on the theoretical premises and socio-political conditions, education is treated as: a process of human permanent life-long learning: the right and, at the same time, civic duty of a human and a social imperative; an instrument of political power to meet specific social, political party-related, union, national, cultural interests and goals; the area of social self-regulation, the main factor in the development of human capital, the quality of life of societies or civilization: a type of symbolic

informacyjnego, Warszawa 2015; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

2 Tym terminem określa się zwykle ogół narzędzi sprzętowych i programowych związanych z technikami gromadzenia, przetwarzania, przesyłania i udostępniania informacji, wykorzystywanych przez ludzi do pozyskiwania wiedzy oraz do komunikacji z innymi ludźmi. ##This term is usually used to describe all hardware and software tools related to techniques for gathering, processing, transmitting and sharing information used by people to acquire knowledge and to communicate with other people. ##Najważniejszym, chociaż nie jedynym, składnikiem cyberprzestrzeni jest obecnie internet. The most important, though not the only, component of cyberspace is currently the internet.

3 W. Okoń, *Nowy słownik pedagogiczny*, Warszawa 2012, s. 44.

violence imposing the culture of the dominant group on the representatives of other social groups, thus, the factor of social stratification, which generates mechanisms and opportunities for social promotion as well as selection and marginalization; a "screen of culture" explaining the complexity of its field of meanings and symbols; type of a normative discourse, presenting particular mental perspective, enabling one to take sides with world-view, ideological or moral conflicts[4].

Relationships between cyberspace security and education can be described at different levels that are interrelated. The starting point is the importance of security of the individual (personal security). Shaping of a man in the education process - regardless of whether it is institutionalized (school, police, fire, city, army, workplace, etc.) or natural (in the family, in the closer and more distant social environment) or by self-education – is aimed at helping a human individual to know and understand himself, to know and understand the world of cyberspace surrounding him, to develop his own abilities and interests, to shape his own character, worldview, and attitudes towards himself and cyberspace.

Cyber security is one of the elements of the security system of a state. Nowadays it occupies an important role within this system and is a dynamically developing field[5].

4 B. Suchodolski, S. Mazur, *Edukacja dla bezpieczeństwa. Materiały międzynarodowej konferencji naukowej*, Katowice 2015, s. 26.

5 W przedmiocie bezpieczeństwa, w tym bezpieczeństwa państwa, zob. szerzej: M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016; M. Karpiuk, K. Prokop, P. Sobczyk, *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013; W. Kitler, M. Czuryk, M. Karpiuk (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013; M. Karpiuk, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017; M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014; M. Bożek, M. Karpiuk, J. Kostrubiec, *Zasady ustroju politycznego państwa*, Poznań 2012; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2; M. Karpiuk, *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.

The purpose of the article is to characterize the most important threats lurking in cyberspace and affecting the level of personal and structural security, as well as presenting ways (challenges) of using various forms and methods of security education to counteract these threats.

Cyber threats targeting man

Unfortunately, as cyberspace becomes a virtual reflection of the physical reality, negative forms of human activity penetrate it as well. Created to enable scientific cooperation, the internet network gives a great sense of anonymity, and it is used by criminals, terrorists, as well as some countries to conduct illegal activities or aggression against other entities.

Threats related to cyberspace concern the possibility of information theft (which exposes the robbed site to losses), the possibility of intentional and illegal change of information (which disturbs this sphere of professional or private activity that depends on the accuracy and timeliness of information which has changed), the possibility of limiting access to information up to and including complete blocking (which may paralyze certain spheres of action with sometimes catastrophic consequences), etc. The number of threats to which every cyberspace user may be exposed is very large, and the scale of their harmfulness is constantly increasing due to the phenomenon of increasing migration to cyberspace, so, in order to give further considerations a more specific dimension, we will briefly assess the scale of this migration.

Generally, the source of threats in cyberspace can be technology or people. The threats posed by the technology are obviously serious, because a computer failure can disable the activities of an important institution (for example, a bank), depriving it of the expected profits and prestige.

In any IT system, even after a short time of its operation, a situation arises that the data stored in the computer's memory is worth much more than the computer alone. Meanwhile, this data may be lost due to a technical failure (physical damage to the disk), due to a faulty software or due to the erroneous actions of people operating the system.

Human-generated damage and threats in cyberspace arise from a variety of reasons. The most important of them include: 1) reading someone else's letters for fun; 2) testing the security of foreign systems, theft of information; 3) understanding the strategic secrets of competitors; 4) willingness to improve one's own image and prestige; 5) embezzlement of the company

money; 6) revenge for getting laid off; 7) interception of credit card numbers; 8) getting to know military and industrial secrets.

To describe the conflict situation involving net work organizations, the name "network war", defined as "emerging form of social conflict (and crime), less intense than traditional armed struggle, in which protagonists use network forms of organizations and related doctrines, strategies and technologies adapted to the information age"[6] has been employed. As B. Bolechów emphasizes: "characteristic for the conflicts fought by networks is the blurring of divisions, which hierarchical structures generally consider to be very important. The boundaries between what is external and internal, what is legal and illegal, criminal and military, related to war and peace, private and public are becoming less clear. Similarly, the border between defensive and offensive actions becomes blurred (the network actors may, for example, attack in the name of a defense or, defending at the strategic level, attack at the tactical level), or between violence and influence (cyber terrorism is such a border phenomenon – it seems to be more connected with disruptive rather than destructive actions). Blurring borders may cause helplessness and paralysis of traditional hierarchical structures, in which areas of competence are determined according to clear divisions. Meanwhile, the opponent (in addition to functioning on a transnational level) also operates in the internal "gray areas", in which the competences of individual hierarchical structures overlap or are not included, which leads to a clinch or competence gap, respectively"[7].

The internet creates new communication possibilities and is the pillar of the modern network society. It provides its users with opportunities: creating networks, creating social relations, expressing opinions, creating social movements, managing projects. At the same time, it also creates new challenges related to freedom, information processing, forms of employment, and possible exclusion from the network. Network society influences various areas of human life – among some it raises fear and questions about education, employment, lifestyles, social inequalities, while others see it as an opportunity

6 J. Arguilla, D. Ronfeldt, *The Aduent of Netwar* [w:] J. Arguilla, D. Ronfeldt (red.), *Networks and Netwars. The Future of Terror, Crime and Militancy*, Santa Monica 2001, s. 9.

7 B. Bolechów, *Sieci przeciwko hierarchiom – wyzwania dla suwerenności państw* [w:] Z. Leszczyński, S. Sadowski (red.), *Suwerenność państwa we współczesnych stosunkach międzynarodowych*, Warszawa 2005, s. 165.

and hope for better organization of their own lives. Network society raises new challenges people have to confront.

Cyberspace is also used by terrorists as a tool for conducting politically motivated activities. Due to controversy and problems with a clear definition of the concept of cyberterrorism, it is difficult to unequivocally classify specific examples of attacks as the effect of terrorist activities in cyberspace. Many incidents attributed to terrorists may be a form of vandalism, covertly sponsored or secretly accepted by the state, which is difficult to prove.

Emerging new grounds of cyberterrorism are primarily the result of the evolution of conflicts from traditional and industrial ones to the conflicts of the post-industrial era, in which the trigger is not so much frustration arising out of the lack of access to material goods, but rather the issues of participation in the increasingly more important pool of social goods- the new participants, primarily groups of professionals are their feature.

Terrorist attacks on the internet, hacker attempts to intercept data or block websites, and other constantly evolving ICT activities aiming at depriving control of or taking over the information seem to be potentially real. Does this mean that in the near future the e-mail bomb will be a greater threat than conventional weapons, and cyberwar will become the greatest danger to the global village? In the face of globalization, cyberspace protection has become one of the basic strategic goals in the field of each country's security. In the age of free flow of people, goods, information and capital – the security of a democratic state depends on the development of mechanisms to effectively prevent and combat threats to the security of cyberspace. It is necessary to develop national solutions in a coordinated way to prevent and combat emerging threats, in particular to respond quickly and efficiently to attacks directed against systems, ICT networks and services offered on the web or services which use it.

The need for qualified staff that can effectively fight the ever-changing forms of activities in cyberspace deserves to be emphasized. Over the next few years, the importance of the information environment and security in this area will definitely grow and become one of the priorities in adjusting mechanisms ensuring national security.

Challenges of security education in the area of cyberspace

In connection to contemporary threats, there appears a tendency outlined by T. Borowska, which refers to the needs of the educational preparation of the human individual to deal with various threats, mainly through the development of his ability to create his own existence. The author claims that moral, cognitive and emotional resources can have creative power, which, thanks to education, may be acquired by "homo construens – a building man"[8]. The core of these resources are values, especially freedom and responsibility, allowing the "building man" to go beyond the boundaries of his own life in the conditions of threats arising from both the real world (stress) as well as the world of illusion created by the technical media. The illusory world of techno culture is according to T. Borowska one of the main sources of threats and stress, causing negative human reactions and having a destructive effect on all areas of his psychosocial functioning. This especially concerns anxiety, stress and various emotional disorders[9].

Education for safety in cyberspace should consist in: defense training for managerial staff, departmental training and general defense training for the entire society. Due to the objective occasional occurrence of emergencies, modern countries establish universal rescue systems. Such systems are common for the times of peace and war. The base of the systems are functioning rescue services. Concepts are prepared for managing the state and individual regions in a situation of crisis.

In individual areas of security in cyberspace, it is necessary to appoint leaders and institutions specializing in the accumulation of knowledge (theoretical and practical) in a given scope and coordination of activities of all the elements of the defense and protection subsystem. This applies in particular to: 1) combating terrorism, including monitoring international terrorism, general and specific prevention on the country's territory, protection of critical infrastructure, training of units intended to actively combat terrorist

8 T. Borowska, *„Homo construens" – człowiek budujący. Edukacyjne przygotowanie do radzenia sobie z różnymi zagrożeniami* [w:] J. Gnitecki, J. Rutkowiak (red.), *Pedagogika i edukacja wobec nadziei i zagrożeń współczesności. Materiały z III Ogólnopolskiego Zjazdu Pedagogicznego*, Warszawa–Poznań 1999, s. 351.

9 Zob. T. Borowska, *Następstwa zagrożeń występujących w życiu człowieka. Zamówienia składane edukacji wynikające z eksploracji współczesnej psychiatrii oraz psychologii* [w:] A. Siemak-Tylikowska, H. Kwiatkowska, S.M. Kwiatkowski (red.), *Edukacja nauczycielska w perspektywie wymagań zmieniającego się świata*, Warszawa 1998.

acts, as well as methods and procedures for preparing the population in the event of an act of terrorism. This requires establishment of a new act on combating terrorism; 2) combating organized crime, with a precise definition of the leading role of the National Security Bureau in the execution of this task. Today, there exist areas of crime in which almost all entities are interested.

It is necessary to establish a public-private cooperation platform for combating cybercrime, as well as to develop (change) the legal regulations specifying the obligations and powers of its members, to indicate sources of financing, to determine the rules for the national and international cooperation (interinstitutional and cross-border approach), including assessment of the amount of data processed and an indication of technical solutions for this platform.

It seems reasonable to specify the methodology and clear criteria for the selection of topics in scientific and research work in the field of security in cyberspace. A database of experts and research centers should be created which have the potential and resources to support the activities of entities responsible for security in cyberspace with their knowledge.

Education for security in cyberspace consists in numerous cognitive and empirical areas subject to many analyses. These are didactic and educational processes covering education and upbringing as well as broadly understood education, aiming at proper preparation of young people and adults for threat situations from cyberspace. Challenges and threats are listed as the main problem (research) areas, as well as subjective and objective security structure. New areas are also emerging in research in the area of education for security – including: determining the nature and legitimacy of respecting the human tolerance to risk and uncertainty; shaping and developing the human ability to work on anxiety and fear; building skills in dealing with one's own and other people's emotions; broadening the perspective of a person involved and exposed to threats.

The structural arrangement and organisation of institutions which directly affect education for security also require changes. These changes should mainly concern normative and organisational issues in the field of cooperation and removal of the effects of threats. It seems appropriate to start from constitutional foundations and security strategies concerning social needs.

The media should systematically participate in raising public awareness in the field of security, existing threats and methods to prevent them. Due to the widespread and common access of recipients to public television, it

is necessary to conduct educational and preventive programs utilising to promotie knowledge about security.

Education for safety should be a continuous process aiming at the most comprehensive development of personality and general mental fitness. An individual, improving his personality by deepening knowledge, fulfills himself as a human person. Knowledge, skills as well as his moral and spiritual values are values in themselves related to the realisation of his potential.

Many educators, including educators in the area of safety, give consideration to a model of the 21st century man. They draw attention to the need to develop the characteristics of the individual and to realize their ambitions in a way that does not harm the society. Hence, individual and social development is needed – it is a modern education model that should have many features, including: 1) people (youth, adults) being educated in a modern way, that are being educated for the future; 2) that are able to solve problematic tasks; 3) that can counteract all threats; 4) that can direct the development of their personality; 5) that would be able to use their knowledge in the near and distant future.

Education for the safety of modern man must be based on universal, national, social and personal values. From this arises the need to defend peace, to protect the natural environment, and to strive to adhere to certain principles in one's life. It should be noted that the hierarchy of values has been shaken recently and the life goals and priorities of many citizens have changed. The current customary and even legal norms are questioned and new forms of social dysfunctionalities are developing. It is worth to pay attention to the praxeology of education for security.

Greater emphasis should be placed on developing young people's ability to recognize the wide-ranging threats and dangers of cyberspace around them.

School education should include time and space for shaping young people's awareness of the possibility of cyber-terrorist threats. Educational institutions should focus on providing reliable knowledge about threats in cyberspace, shaping the attitude of civic vigilance, showing a broad context of security considerations.

The perspective of multilateral education for safety is clearly being developed, and its main subject is the complex process of human development that occurs under the influence of education, and not only school teaching and learning. Reflections on human development concern both the development of the individuals subjected to education and the development of the entire – young and old – generation, in a specific way affecting the development and progress in the society's life.

While analyzing the discussed threats, it is easy to see that information resources and elements of Poland's ICT infrastructure are subject to the same trends as cyberspace at the global level. Along with the progressing computerization of the state, it is necessary to create effective preventive, technical, organisational and legal solutions to protect its citizens.

To achieve these goals, it is necessary to take multi-level actions requiring the cooperation of all interested parties. First of all, appropriate legal norms should be ensured, allowing the effective operation of the state and its institutions in the field of cyberspace security.

Technical issues are another area that requires action. Ensuring cyberspace security will not be possible without developing early warning systems for attacks, implementing additional preventive solutions and special protection for key ICT systems, combined with exercises to assess the resistance of this infrastructure to cyber attacks.

Ensuring the security of cyberspace will not be possible without the involvement of the widest possible group of global network users who, aware of the dangers, will be able to contribute to the protection of this environment. It is necessary to train ICT security specialists and clerical staff consistently.

Bibliography

Arguilla J., Ronfeldt D., *The Aduent of Netwar* [w:] J. Arguilla, D. Ronfeldt (red.), *Networks and Netwars. The Future of Terror, Crime and Militancy*, Santa Monica 2001.

Bolechów B., *Sieci przeciwko hierarchiom – wyzwania dla suwerenności państw* [w:] Z. Leszczyński, S. Sadowski (red.), *Suwerenność państwa we współczesnych stosunkach międzynarodowych*, Warszawa 2005.

Borowska T., *„Homo construens" – człowiek budujący. Edukacyjne przygotowanie do radzenia sobie z różnymi zagrożeniami* [w:] J. Gnitecki, J. Rutkowiak (red.), *Pedagogika i edukacja wobec nadziei i zagrożeń współczesności. Materiały z III Ogólnopolskiego Zjazdu Pedagogicznego*, Warszawa–Poznań 1999.

Borowska T., *Następstwa zagrożeń występujących w życiu człowieka. Zamówienia składane edukacji wynikające z eksploracji współczesnej psychiatrii oraz psychologii* [w:] A. Siemak-Tylikowska, H. Kwiatkowska, S.M. Kwiatkowski (red.), *Edukacja nauczycielska w perspektywie wymagań zmieniającego się świata*, Warszawa 1998.

Bożek M., Karpiuk M., Kostrubiec J., *Zasady ustroju politycznego państwa*, Poznań 2012.

Chałubińska-Jentkiewicz K., Karpiuk M., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016.

Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4.

Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014.
Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.
Karpiuk M., *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2.
Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.
Karpiuk M., Chałubińska-Jentkiewicz K., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.
Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.
Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.
Kitler W., Czuryk M., Karpiuk M. (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013.
Okoń W., *Nowy słownik pedagogiczny*, Warszawa 2012.
Suchodolski B., Mazur S., *Edukacja dla bezpieczeństwa. Materiały międzynarodowej konferencji naukowej*, Katowice 2015.

Zagrożenia i wyzwania człowieka w cyberprzestrzeni a jego edukacja

Streszczenie

Współczesny człowiek mocno akcentuje potrzebę bezpieczeństwa we wszystkich aspektach życia społecznego i indywidualnego. Treść artykułu dotyczy zagrożeń i wyzwań człowieka w cyberprzestrzeni. Autor pokazuje w nim związki i zależności pomiędzy bezpieczeństwem a edukacją. Wiele miejsca poświęca charakterystyce zagrożeń w cyberprzestrzeni. Wobec dynamicznie zmieniającej się rzeczywistości, szczególną uwagę autor nakazuje zwrócić na nowoczesne sposoby przeciwdziałania zagrożeniom płynącym z cyberprzestrzeni. Teść artykułu pokazuje jak istotnym aspektem życia człowieka jest szeroko pojęta profilaktyka oraz edukacja we wszystkich możliwych etapach korzystania przez człowieka z cyberprzestrzeni.

Słowa kluczowe: zagrożenia, wyzwania, edukacja dla bezpieczeństwa, poczucie bezpieczeństwa, człowiek, społeczeństwo, profilaktyka, nauczyciel, media, globalizacja